Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Směrovací protokoly pro IPv6 s využitím směrovačů Huawei

Routing Protocols for IPv6 Using Huawei Routers

2016 **Bc. Ondřej Velička**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Ondřej Velička**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T059 Mobilní technologie

Téma: Směrovací protokoly pro IPv6 s využitím směrovačů Huawei
Routing Protocols for IPv6 Using Huawei Routers

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování směrovacích protokolů pro sítě založené na protokolu IPv6 v laboratorním prostředí s využitím směrovačů Huawei.

Osnova práce:
1. Popište směrovací protokoly, které jsou využívány v sítích založených na protokolu IPv6.
2. Navrhněte a v laboratorních podmínkách realizujte různé druhy sítí IPv6 s využitím směrovačů Huawei. Ověřte funkčnost navržených řešení.
3. Prakticky vyzkoušejte řešení umožňující koexistenci zařízení pro IPv4 a IPv6.
4. Ověřte kompatibilitu směrovačů Huawei a Cisco v testovaných sítích.

Seznam doporučené odborné literatury:

[1] TEARE, Diane, et al. *CCNP Routing and Switching Foundation Learning Library: Foundation Learning for CCNP ROUTE, SWITCH, and TSHOOT (642-902, 642-813, 642-832).* 1st ed. Indianapolis: Cisco Press, 2010. ISBN-13: 978-1-58705-885-1.
[2] Dokumentace k zařízením Huawei a Cisco.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2015
Datum odevzdání: 29.04.2016

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky OSTRAVA

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *25. dubna 2016*

podpis studenta

Poděkování

Rád bych poděkoval Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Abstrakt

Tato diplomová práce se zabývá směrováním a směrovacími protokoly v IPv6 sítích, jež jsou postaveny především na směrovačích společnosti Huawei s doplněním o směrovače společnosti Cisco. Úvodem práce je zmíněna problematika IPv6 protokolu, za jakým účelem vznikl, jak funguje IPv6 adresování, či jak se liší od starší verze IPv4. V další části jsou teoreticky popsány vybrané směrovací protokoly pro IPv6, které jsou podporovány jak směrovači společnosti Huawei, tak směrovači společnosti Cisco. U každého z těchto směrovacích protokolů je popsán princip, vlastnosti, přednosti, možnosti využití a způsob implementace podpory IPv6 protokolu. Ke všem popsaným směrovacím protokolům náleží i praktická část, která obsahuje schéma testované topologie, postup konfigurace a také ověření správné funkčnosti daného protokolu. V neposlední řadě tato práce obsahuje kapitolu věnující se řešením, která umožňují koexistenci zařízení pro IPv4 a IPv6. Závěrem je zhodnocena kompatibilita a popsány rozdíly mezi směrovači Huawei a Cisco.

Klíčová slova

BGP4+; Cisco; Dual Stack; GRE; Huawei; IPv6; IS-IS; kompatibilita; konfigurace; směrovač; směrování; tunely; OSPFv3; RIPng

Abstract

This thesis is concerned with routing and routing protocols in IPv6 networks that are mainly built on Huawei routers with addition of Cisco routers. Introduction of the thesis is concentrated on IPv6 protocol problems, for what purpose was the protocol created, what are IPv6 addressing functions or how IPv6 protocol differs from older version IPv4. Selected routing protocols for IPv6 that are supported by Huawei routers as well as Cisco routers are theoretically described in the next part of the thesis. The principle, features, advantages, possibilities of the use and support implementation of IPv6 protocol are described in each of these routing protocols. All described routing protocols include a practical part that contains a diagram of tested topology, configuration procedure and verification of correct functioning of the protocol too. The thesis contains a chapter dedicated to solutions that enable coexistence of devices for IPv4 and IPv6. In conclusion, compatibility evaluation and description of differences between Huawei and Cisco are contained.

Key words

BGP4+; Cisco; compatibility; configuration; Dual Stack; GRE; Huawei; IPv6; IS-IS; OSPFv3; RIPng ; router; routing; tunnels

Seznam použitých zkratek

Zkratka	Anglický význam	Český význam
6rd	IPv6 rapid deployment	Automatický tunelovací mechanismus
6to4	Connection of IPv6 Domains via IPv4 Clouds	Automatický tunelovací mechanismus
6VPE	IPv6 VPN Provider Edge Router	Mechanismus přenosu IPv6 komunikace přes MPLS VPN síť
ABR	Area Border Router	Hraniční směrovač oblasti směrovacího protokolu OSPF
AFI	Address Family Identifier	Identifikátor adresní rodiny
AS	Autonomous System	Autonomní systém je větší část sítě se společnou směrovací politikou a správou
ASBR	Autonomous System Border Router	Hraniční směrovač autonomního systému OSPF
ASE	Autonomous System External	Nese parametry o externích cestách v systému OSPF
ASN	Autonomous System Number	Číslo autonomního systému, přidělováno organizací IANA
BGP	Border Gateway Protocol	Směrovací protokol využívaný ke směrování mezi AS
BGP4+	Border Gateway Protocol version 4+	Novější verze směrovacího protokolu umožňující směrování IPv6 provozu
CIDR	Classless Inter-Domain Routing	Metoda směrování, pomocí které lze rozdělit velké sítě na podsítě
DHCP	Dynamic Host Configuration Protocol	Protokol pro automatickou konfiguraci parametrů nutných ke komunikaci pomocí IP protokolu
DEC	Digital Equipment Corporation	Společnost, která vyvinula směrovací protokol IS-IS
DNS	Domain Name System	Hierarchický systém doménových jmen
EBGP	External Border Gateway Protocol	Vazba mezi BGP směrovači v různých AS
EGP	Exterior Gateway Protocol	Třída směrovacích protokolů ke směrování mezi AS
FTP	File Transfer Protocol	Protokol umožňující přenos souborů přes počítačovou síť
GRE	Generic Routing Encapsulation	Protokol určený k tunelování paketů přes síť pomocí techniky zapouzdření
IANA	Internet Assigned Numbers Authority	Organizace dohlížející na přidělování IP adres a správu DNS zón po celém světě

IBGP	Internal Border Gateway Protocol	Vazba mezi BGP směrovači uvnitř jednoho AS
ICMP	Internet Control Message Protocol	Protokol umožňující ověřit dostupnost konkrétních prvků v síti protokolu IPv4
ICMPv6	Internet Control Message Protocol Version 6	Protokol umožňující ověřit dostupnost konkrétních prvků v síti protokolu IPv6
IETF	Internet Engineering Task Force	Organizace, která vyvíjí a podporuje internetové standardy
IGP	Interior Gateway Protocol	Třída směrovacích protokolů ke směrování uvnitř AS
IP	Internet Protocol	Internetový protokol pracující na síťové vrstvě ISO/OSI modelu
IPv4	Internet Protocol version 4	Internetový protokol čtvrté verze
IPv6	Internet Protocol version 6	Internetový protokol šesté verze
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol	IPv6 přestupní mechanismus pro přenos IPv6 paketů nad IPv4 sítí
IS-IS	Intermediate System to Intermediate System	Směrovací protokol pro směrování uvnitř AS
L1	Level 1	Oblast první úrovně směrovacího protokolu IS-IS
L2	Level 2	Oblast druhé úrovně směrovacího protokolu IS-IS
LS	Link State	Třída směrovacích protokolů vybírajících nejkratší cestu podle její ceny (stavu)
LSA	Link State Advertisement	Hlavní komunikační zpráva protokolu OSPF
LSDB	Link State Database	Zprávy směrovacího protokolu OSPF obsahující informace o topologii AS nebo oblasti
MAC	Media Access Control	Fyzická adresa identifikující síťové zařízení
MD5	Message Digest algorithm 5	Kryptografická hašovací funkce
MTU	Maximum transmission unit	Označení maximální velikosti IP datagramu, který lze odeslat do sítě
NAT64	Network Address and Protocol Translation from IPv6 clients to IPv4 servers	Přechodový mechanismus umožňující IPv6 klientům přistupovat k IPv4 serverům
NET	Network Entity Titles	Adresy prvků využívané směrovacím protokolem IS-IS
NIR	National Internet Registry	Organizace koordinující přidělování IP adres na národní úrovni

NLPID	Network Layer Protocol Identifier	Identifikátor protokolu síťové vrstvy ISO/OSI modelu
NLRI	Network Layer Reachability Information	Pole aktualizační zprávy směrovacího protokolu BGP4+ obsahující informace o dosažitelných cestách v podobě prefixu a jeho délky
NSSA	Not-So-Stubby-Area	Typ OSPF oblasti, umožňuje přenášet LSA zprávy typu 7 informující o externích cestách
OSPF	Open Shortest Path First	Směrovací protokol pro směrování uvnitř AS
OSPFv3	Open Shortest Path First Version 3	Směrovací protokol pro směrování uvnitř AS podporující IPv6 protokol
RIP	Routing Information Protocol	Směrovací protokol pro směrování uvnitř AS podporující IPv6 protokol
RIPng	Routing Information Protocol next generation	Směrovací protokol pro směrování uvnitř AS podporující IPv6 protokol
RIR	Regional Internet Registry	Organizace starající se o přidělování IP adres a čísel AS na kontinentální úrovni
RTE	Route Table Entry	Zpráva směrovacího protokolu RIPng, obsahuje informace o připojených sítích
SAFI	Subsequent Address Family Identifier	Poskytuje dodatkovou informaci o typu NLRI
Teredo	Teredo	Automatický tunelovací mechanismus pro IPv6 pakety přes IPv4 síť
TLV	Type-length-value	Formát dat využívaný například u směrovacího protokolu IS-IS
TCP	Transmission Control Protocol	Protokol transportní vrstvy TCP/IP, spojově orientovaný, spolehlivý
UDP	User Datagram Protocol	Protokol transportní vrstvy TCP/IP, orientovaný na zprávy, nespolehlivý

Obsah

Úvod

Žijeme ve století digitalizace? V minulém století vznikly nejprve počítače, které byly na počátku velmi jednoduché a dovolovaly lidem provádět pouze základní výpočty a jednoduché operace. S postupem času se však naučily provádět mnohem složitější algoritmy a výpočty, a to stále rychlejším tempem. Netrvalo to dlouho a vznikl Internet. Ten však na jeho počátku propojoval pouze pár počítačů, které si byly schopny posílat jednoduché zprávy. Jak se rozšíření počítačů a jejich využití zvyšovalo, rostl i Internet a služby, které poskytoval. Ačkoliv se počítače neustále zmenšují, jejich výkon neustále roste. Proto je v dnešní době najdeme téměř všude – uvnitř chytrých hodinek, telefonů, tabletů, tiskáren, televizí, ledniček, osvětlení, dopravního značení a uvnitř mnoho dalších zařízení a věcí. Zkrátka se digitalizuje téměř vše. Toto se ovšem neděje pouze kvůli počítačům a tomu, že nám to jejich parametry dovolují. Velkou mírou je za to zodpovědný právě Internet, jehož rozšíření je v dnešní době téměř po celém světě, a pomocí kterého lze tato nejrůznější zařízení například vzdáleně ovládat, spravovat, získávat z nich data, či na nich data zpracovávat.

S tímto obrovským rozšířením využití elektroniky v posledních letech přišel i problém – nedostatek IP adres. V době vzniku protokolu IPv4 (1981), který se jako první hromadně rozšířil, jeho tvůrci nepředpokládali, jak rychle se bude zvětšovat počet zařízení využívající tento protokol, a tak počet unikátních adres, pomocí kterých se Internet řídí, byl omezen zhruba na 4 miliardy zařízení. V průběhu používání protokolu IPv4 byly vyvinuty různé technologie pro „šetření“ IPv4 adres, které měly odvrátit jejich vyčerpání. Nicméně počátkem devadesátých let 20. století bylo zřejmé, že i přes všechny snahy dojde k vyčerpání adresního prostoru protokolu IPv4, a tak organizace IETF do roku 1996 vytvořila novou verzi internetového protokolu, která je označována jako IPv6. Adresní prostor verze 6 je extrémně velký, a teoreticky nabízí více než bilion adres na čtvereční centimetr povrchu planety Země. Změn v této verzi je celá řada, a aby mohl být protokol IPv6 využíván v praxi, bylo potřeba upravit některé stávající či vytvořit několik nových protokolů a zařízení, které umí s protokolem IPv6 pracovat. Změny a vývoj nových protokolů se dotkl i kategorie protokolů určených ke směrování paketů v síti. Jedná se o nové verze již používaných směrovacích protokolů pro IPv4. Některé byly pouze upraveny, jiné zcela předělány, a tak vznikly směrovací protokoly pro IPv6 – RIPng, OSPFv3, IS-IS a BGP4+. Jak tyto protokoly pracují, na jakém principu je založena jejich funkce, jak je u nich řešena podpora IPv6, či jak spolupracují se zařízeními společnosti Huawei včetně ověření ve školní laboratoři na reálných topologiích je hlavním tématem této diplomové práce.

Proces přechodu z IPv4 na IPv6 je možné označit během na dlouhou trať. Vzhledem k rozlehlosti Internetu a nákladnosti přechodu z IPv4 na IPv6, není možné tuto změnu provést během jednoho dne, či několika let. Z toho důvodu bylo vyvinuto několik druhů mechanismů a zařízení, které umožňují současný běh obou protokolů zároveň. Většina z těchto mechanismů funguje na principu tunelování paketů jednoho protokolu napříč druhým a naopak. Principy řešení koexistence protokolů IPv4 a IPv6 jsou jedním z témat, kterým se tato diplomová práce věnuje. V současné době se podle statistik společnosti Google počet uživatelů využívajících její služby skrze protokol IPv6 pohybuje na hranici 10%.

1 Směrovací protokoly pro IPv6

1.1 Protokol IPv6

Internetový protokol verze 6 je poslední a nejnovější verzí tohoto protokolu. Je to komunikační protokol, který poskytuje identifikační a lokační systém pro počítače v sítích a komunikační cesty pro přenos dat skrz Internet. IPv6 byl vytvořen organizací IETF (Internet Engineering Task Force) z důvodu vyčerpání adresního prostoru starší verze tohoto protokolu, a to IPv4. Nová verze protokolu by měla postupně nahradit jeho starou verzi. Podle statistik získaných v květnu roku 2014 se pomocí protokolu IPv4 řídilo více než 96 % internetového provozu po celém světě. Nicméně během února stejného roku byla poprvé překročena hranice 3% uživatelů využívajících služby Google skrze protokol IPv6. Nyní na počátku roku 2016 se toto číslo pohybuje na hranici 10%.

1.1.1 Adresa IPv6

Každému zařízení připojenému do sítě Internet je přiřazena IP adresa pro jeho identifikaci a definici umístění. S narůstajícím počtem nových zařízení připojených k Internetu nastal problém omezeného počtu IP adres, které protokol IPv4 nabízí.

Protokol IPv4 využívá 32-bitových adres a celkem nabízí:

$2^{32} \cong 4{,}3$ miliard adres

Protokol IPv6 využívá adresy délky 128-bitů a nabízí:

$2^{128} = 3{,}4 \times 10^{38}$ adres

Tyto dvě verze protokolů mezi sebou nespolupracují, což poměrně značně komplikuje nasazení nové verze protokolu do užití. Jedinou možností jak novou verzi postupně zavést do sítě Internet je postupnou výměnou starých zařízení za nová, která podporují obě verze protokolu, a tak dokáží pracovat s protokolem IPv4 i IPv6 najednou. Takováto zařízení se označují názvem "dual stack". Nárazová změna protokolu z IPv4 na IPv6 není možná, a to z důvodu rozsáhlosti Internetu a jeho každodenního využívání stovkami miliónů uživatelů po celém světě.

[1]

1.1.2 Styly zápisu IPv6 adresy

IPv6 adresa je reprezentována jako 8 skupin čtyř hexadecimálních číslic oddělených dvojtečkou.

Plný tvar:
FF01:0000:0000:0000:0000:0000:0000:0101

Vypuštění úvodních nul:
FF01:0:0:0:0:0:0:101

Vypuštění souvislých sekvencí 4 nul a nahrazení za :: lze jen jednou pro zachování jednoznačnosti.
FF01::101

[2]

1.1.3 Třídy adres IPv6

Podobně jako u staré verze protokolu, i zde jsou adresy roztříděny podle toho, kolik zařízení adresují. Proto je můžeme zařadit do tří základních skupin:

- Unicast - neboli adresa, která označuje a patří jen jednomu zařízení v síti. Internetový protokol tudíž doručí paket přímo této jediné adrese.
- Anycast - adresa, která je přiřazena skupině rozhraní, většinou různých uzlů. Paket zaslaný na tuto adresu je doručen pouze jednomu rozhraní z celé skupiny, obvykle tomu nejbližšímu k odesílateli na cestě skrze síť. Tento typ adres nelze jednoznačně identifikovat, jelikož mají stejný formát jako adresy předešlého typu.
- Multicast - adresa využívána několika zařízeními zároveň. Paket zaslaný na tuto adresu je doručen všem zařízením, které jsou členy této skupiny neboli multicast adresy.
  Rozsah adres FF00::/8 je rezervován pro účely multicastu – prvních osm bitů adresy jsou pouze jedničky – 1111 1111. Multicast může být poslán na různé rozsahy adres. Přehled těchto rozsahů je v následující tabulce.

[3]

Tabulka 1.1: Prefixy pro multicast použité v protokolu IPv6. [3]

Prefix	**Rozsah**
FF02::	Link local: všechny uzly ve stejné LAN
FF05::	Site local: určená pro celou samostatnou síť.
FF08::	Organization scope: určen pro mnohem větší sítě uvnitř velkých organizací.
FF0e::	Global scope: globální rozsah, definován organizací IANA.
FF01::	Interface local: samotné rozhraní uzlu; využití pro přenos loopbacku pro multicast

Jak je možné zaznamenat, chybí zde třída broadcast. Funkce těchto adres byla nahrazena adresami třídy multicast, viz výše.

1.2 Směrovací protokol RIPng

Protokol RIP příští generace (RIPng) patří mezi IGP protokoly, což jsou směrovací protokoly využívané ke směrování mezi výchozími bránami (nejčastěji směrovači) v rámci jednoho autonomního systému. Stejně jako jeho verze pro IPv4 patří do třídy tzv. „distance vector„ protokolů, které používají k výpočtu nejkratší vzdálenosti v síti algoritmus založený na základě počtu „přeskoků“ přes jednotlivé směrovače na trase. Informace o směrování, které si směrovače mezi sebou vyměňují, a jsou používané k výpočtům cest v síti, jsou určené pro protokol IP verze 6. Z tohoto důvodu není směrovací protokol RIPng zpětně kompatibilní s protokolem RIPv2, který pracuje s adresami směrovacího protokolu IPv4.

Pro výpočet nejkratších cest v síti používá tento směrovací protokol Bellmanův-Fordův algoritmus. Ten vypočítá metriku do jednotlivých sítí na základě počtu nezbytných přeskoků. Protokol RIPng je určený k tomu, aby fungoval jako IGP protokol především pro menší sítě. Komunikaci mezi směrovači provádí na UDP portu 521. Podporuje více IPv6 adres na každém rozhraní.

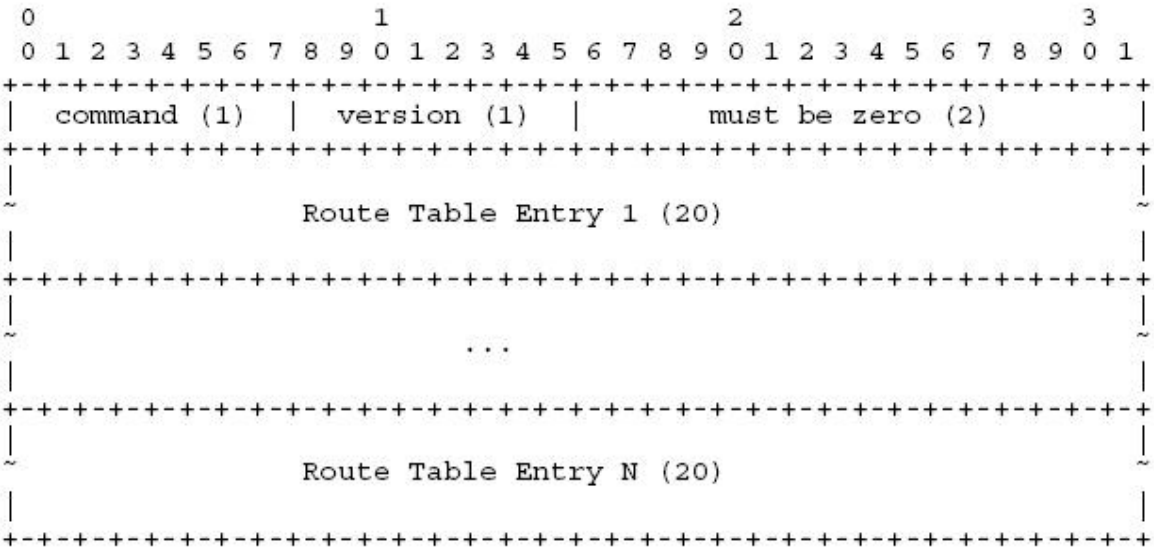
Protokol má následující omezení:

- Metrika může být 1 až 15. To znamená, že nejdelší cesta v síti se směrovacím protokolem RIPng nesmí překročit 15 skoků. Každý skok (směrovač, přes který paket musí na cestě k cíli projít) má hodnotu 1.
- Po rekonstrukci směrovací tabulky je náchylný k tvorbě směrovacích smyček v síti. Zvláště v případech, kdy je implementován v rozlehlých sítích, které jsou postaveny z několika stovek směrovačů. Čas, který protokol RIPng potřebuje k odhalení smyček v síti, může být velice dlouhý.
- Pro určení nejkratší cesty využívá metriku založenou na počtu směrovačů, přes které je nutno projít na trase k cíli. Ostatní protokoly z řady IGP využívají pro určení nejkratší cesty v síti dodatkových parametrů, jako je například rychlost linky, spolehlivost a zátěž.

[4]

1.2.1 Formát RIPng zprávy

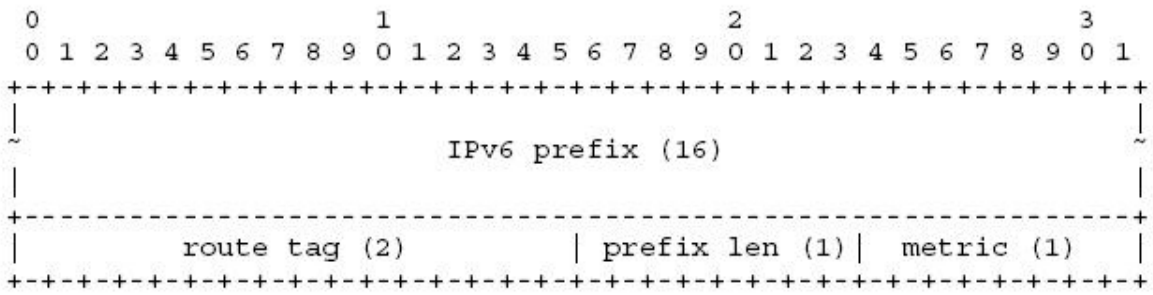
Každý směrovač používající RIPng jako protokol ke směrování, má spuštěný směrovací proces, který odesílá a přijímá datagramy (informace o směrování v dané síti) na portu UDP 521. Každá zpráva obsahuje hlavičku RIPng ve formátu (viz obrázek 1.1).



Obrázek 1.1: Formát hlavičky paketu RIPng. Velikost polí je zobrazena v bajtech. [5]

- **Command** – Určuje, zdali je paket žádostí nebo odpovědí. Žádosti jsou zasílány ostatním směrovačům pro získání informací o síti. Zprávy typu odpověď jsou zasílány periodicky anebo v okamžiku, kdy je přijata žádost od jiného směrovače. Periodické odpovědi jsou nazývány aktualizacemi. Tyto aktualizační zprávy obsahují pole *command*, *version*, spolu s polem *destination* a *metric*.
- **Version** – Udává verzi protokolu RIPng, který je spuštěn na původním směrovači. V současnosti se udává verze 1.

Zbylá část paketu obsahuje takzvané záznamy směrovací tabulky (RTE), které obsahují informace o sítích, nutné k sestavení směrovací tabulky. Každá zpráva RTE je v následujícím formátu:



Obrázek 1.2: Formát RTE zprávy. Velikost polí je zobrazena v bajtech. [5]

- **IPv6 prefix** – 128 bitů dlouhé předčíslí cíle.
- **Route tag** – je atribut cesty v síti, který musí být propagován a přeposílán s cestou. V případě, jsou-li cesty přeposílány mezi autonomními systémy přes takzvaný EGP protokol, je tento atribut primárně používán k rozlišení externích RIPng cest od cest interních.

- **Prefix len** – významná část předčíslí. Nabývá hodnoty mezi 0 a 128. Bere se z levé strany předčíslí.
- **Metric** – udává aktuální hodnotu metriky, která může být 1 až 15. Metrika 16 je brána jako nedosažitelná síť.

Počet cest zaslaných v aktualizační zprávě, který může být poslán najednou, záleží na středním MTU (Maximum transmission unit), velikosti zprávy RIPng, velikosti RIPng hlavičky a velikosti RTE. [5]

1.2.2 Příští skok

Příští skok (původně next-hop), je udáván speciální RTE zprávou, která se vztahuje ke všem adresovým RTE zprávám, dokud nenastane konec zprávy nebo dokud není připočítán jiný příští skok RTE.

Příští skok je identifikován znaky 0xFF v poli metriky. Pole pro IPv6 předčíslí obsahuje IPv6 adresu příštího skoku. Hodnoty polí *route tag* a *prefix len* jsou nastaveny na 0. Předčíslím příštího skoku by měla být adresa typu link-local odchozího rozhraní, přes které je aktualizace odeslána. Pokud má příští skok nespecifikovanou adresu, znamená to, že příštím skokem je původce propagačních RIPng zpráv.

Periodické aktualizace (výchozí čas je každých 30 sekund) a vyžádané aktualizace musí zůstat v lokální síti. Tyto zprávy by neměly projít skrz směrovač, a proto má IPv6 paket nastavený limit přeskoků na 255. Aktualizační zprávy jsou posílány s cílovou adresou typu multicast FF02::9.

1.2.3 Časování

Pravidelné aktualizace jsou posílány každých 30 sekund každému sousedícímu směrovači. Tyto aktualizace obsahují kompletní směrovací tabulku. Vyžádané aktualizace jsou posílány jako odpověď na žádost nebo v případě změny stavu cesty nebo metriky.

Dalšími dvěma časovači u protokolu RIPng je *timeout* každé cesty a *garbage-collection-timer*. Každá cesta má vyhrazený určitý časový úsek (timeout), po který je považována za platnou. Tento časový limit je spuštěn při sestavení dané cesty a pokaždé, když daná cesta obdrží aktualizaci. V případě, kdy do 180 sekund nedorazí žádná aktualizace pro danou cestu, je tato cesta označena za vypršenou a je spuštěn nový časový limit (garbage-collection-timer), který trvá 120 sekund. Metrika této cesty je rovněž změněna, a to na hodnotu 16, která je brána jako nedosažitelná. Tato cesta bude stále obsahem aktualizací daného směrovače. Pokud vyprší i limit 120 sekund, je tato cesta odstraněna z databáze.

1.2.4 Split Horizon

Jedná se o algoritmus, který zaručuje, aby směrovač neposílal aktualizace cest sousedním směrovačům, od kterých se tyto cesty naučil. Jestli je tato funkce povolena, směrovače si navzájem ignorují aktualizace takovýchto cest.

Variantou této funkce je Split Horizon s atributem Poison Reverse, což znamená, že směrovač takovéto cesty šířit ve svých aktualizacích bude nadále, ale jejich metriku nastaví na nekonečnou (počet skoků=16).

[5]

1.3 Směrovací protokol OSPFv3

OSPFv3 je směrovací protokol pro IP verze 6, tedy dokáže směrovat pakety podle IPv6 adres. Je založený na jeho předešlé verzi OSPFv2, která se využívá pro směrování v IPv4 sítích. Rovněž se tedy jedná o link-state protokol, což znamená, že vybírá nejvhodnější cestu podle stavu linky. Stav linky je u protokolů OSPF vyjadřován cenou linky, což je číslo v rozsahu 1 až 65535. Menší číslo znamená rychlejší/kratší cestu. Informace o směrování rozesílá ostatním směrovačům v síti pomocí zpráv, které se označují zkratkou LSA (Link State Advertisement). Význam této zkratky se dá přeložit jako „propagace stavů linek“.

1.3.1 Rozdíly od OSPFv2

Většina algoritmů používaných v OSPFv2 zůstala stejná. Nicméně, bylo nezbytné provést určité úpravy, ať už kvůli změnám sémantiky mezi IPv4 a IPv6, či jednoduše z důvodu větší velikosti adres pro IPv6.

Jednou z hlavních změn je práce protokolu s linkami, nikoli podsítěmi (angl. subnet), jak tomu bývalo v IPv4 sítích. Protokol IPv6 označuje komunikační prostředek, médium, přes které mohou spolu dva uzly komunikovat na linkové vrstvě jako „linku“. Několik IPv6 podsítí může být přiřazeno jedné lince, přes kterou pak mohou komunikovat dva uzly, ačkoliv nesdílejí jednu společnou IPv6 podsíť. Z tohoto důvodu se u OSPFv3 používá slovní spojení „per-link“ namísto „per-subnet“ jak tomu bývalo u OSPF pro verzi IPv4. Termíny „síť“ a „podsíť“ mohou být v podstatě nahrazeny termínem „linka“. Tato změna má vliv na přijímané OSPF pakety, obsah Hello zpráv a síťových LSA zpráv.

V protokolu OSPFv3 byla odstraněna adresní sémantika z paketů a hlavních LSA zpráv. Především došlo k následujícím změnám:

- IPv6 adresy již nejsou obsaženy v OSPF paketech. Výjimkou jsou pouze LSA zprávy, které jsou přenášeny pakety, které oznamují aktualizaci stavu linky.
- Zprávy Router-LSA a Network-LSA rovněž neobsahují síťové adresy, nýbrž pouze specifikují topologii sítě.
- Identifikátory OSPF protokolu jako jsou ID směrovače, oblasti a LSA zůstávají stejně velké jako u IPv4, a to 32 bitů.
- Sousední směrovače jsou nyní vždy identifikovány pomocí ID směrovače.

Rovněž došlo ke změně rozsahů, kam jsou šířeny LSA zprávy. U OSPFv3 jsou využívány 3 oddělené rozsahy:

- Link-local: LSA je šířeno pouze do lokálních linek, ne dále.
- Oblast: LSA je rozesíláno pouze v rámci jedné OSPF oblasti.

- AS: Zprávy LSA jsou šířeny pouze v rámci jednoho autonomního systému.

[6]

1.3.2 Podpora více instancí na jednom rozhraní

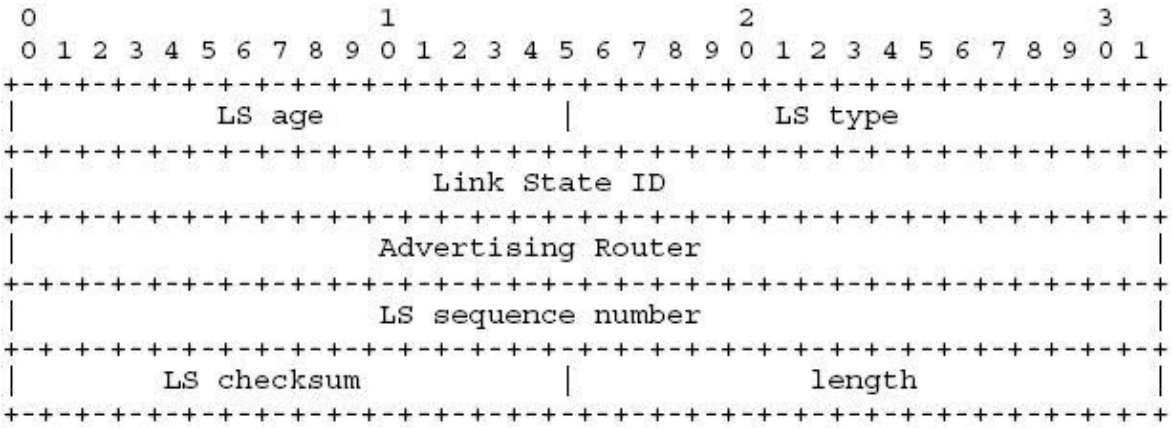
Protokol OSPFv3 nyní podporuje možnost používat více instancí OSPF protokolu na jedné lince. Podpora této funkce je zajištěna novým polem, které bylo přidáno do hlavičky OSPF paketu. Toto pole je nazváno „Instance ID“.

1.3.3 Využití adres typu Link-Local

Tyto adresy jsou využívány na jednotlivých linkách pro potřeby vyhledávání sousedních směrovačů, automatické konfigurace, apod.

1.3.4 LSA zprávy

Všechny LSA zprávy obsahují LSA hlavičku o délce 20 bajtů. Každá z těchto zpráv popisuje a slouží k přenosu informací důležitých pro správnou funkci směrovacího protokolu. Tyto zprávy jsou rozesílány skrze celou směrovací doménu protokolu OSPF. Rozesílání zpráv je spolehlivé, a zajišťuje, že všechny směrovače v síti pracují se stejnými a aktuálními informacemi.



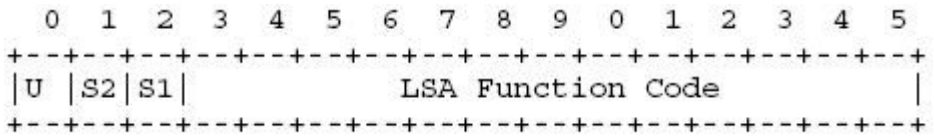
Obrázek 1.3: Hlavička LSA zprávy. [8]

Směrovače si tyto zprávy ukládají do LSDB (Link-State Database), což je databáze stavu linek, resp. informací o topologii sítě. Z této databáze si každý směrovač sestaví svůj strom nejkratších cest, ve kterém hraje roli „kořene“.

Hlavička LSA zprávy obsahuje mnoho informací, které slouží k její unikátní identifikaci.

- **LS Age:** Čas udávaný v sekundách, který uplynul od vytvoření LSA zprávy.
- **Link State ID:** Dohromady s polem *LS Type* a *Advertising Router*, unikátně označuje LSA v LSDB.
- **Advertising Router:** Identifikační číslo směrovače, který vytvořil LSA zprávu.
- **LS Sequence Number:** Slouží k detekci starých nebo duplicitních LSA zpráv.
- **LS Checksum:** Kontrolní součet LSA zprávy zahrnující LSA hlavičku mimo pole *LSA Age*.

- **Length:** Délka zprávy v bajtech včetně hlavičky (prvních 20 bajtů).
- **LS Type:** Toto pole udává funkci dané LSA zprávy, pro kterou je předurčena. První tři bity označují obecné vlastnosti LSA zprávy, zatímco zbylé bity specifikují kód funkce.



Obrázek 1.4: Detail pole LS Type v hlavičce LSA zprávy. [8]

  - **U-** podle tohoto bitu směrovač zachází s neznámou LSA zprávou.
    - **0** = zachází s ní stejně jako se zprávou, která pochází z rozsahu lokální linky.
    - **1** = uloží ji a rozešle dále.
  - **S2 a S1-** určuje rozsah, kam bude LSA rozeslána.

Tabulka 1.2: Kombinace hodnot S2 a S1 v poli LS Type. [8]

S2	S1	Rozsah pro rozeslání
0	0	Link-local
0	1	Area scope
1	0	AS scope
1	1	Rezervováno

  - **LSA Function Code** – definuje specifickou funkci LSA zprávy.

Tabulka 1.3: LSA funkce zprávy. [8]

Kód (LSA Function Code)	Typ (LS Type)	Popis
1	0x2001	Router LSA
2	0x2002	Network LSA
3	0x2003	Inter-Area Prefix LSA
4	0x2004	Inter-Area Router LSA
5	0x4005	AS-external LSA
6	0x2006	Group Membership LSA
7	0x2007	Type-7 (NSSA) LSA
8	0x0008	Link LSA
9	0x2009	Intra-Area Prefix LSA

Stručný popis většiny typů LSA zpráv je uveden v následujícím odstavci:

- **Router LSA**: Každý směrovač v dané oblasti rozesílá tyto zprávy do sítě, aby předal ostatním směrovačům informace o stavu jeho fyzických rozhraní. Tyto zprávy jsou rozesílány pouze v rámci oblasti dané instance směrovacího protokolu.

- **Network LSA**: Shromažďuje a popisuje informace o stavu všech linek a jejich cenách v dané síti, které jsou důležité pro všechny připojené a operující směrovače. Pouze směrovače typu „designated router“ mohou tyto zprávy sledovat a generovat dál do sítě. U protokolu OSPFv3 nenesou tyto zprávy informace o adresách a nejsou závislé na použitém síťovém protokolu.
- **Inter-Area Prefix LSA:** Plní stejnou funkci jako LSA typu 3 u OSPFv2. Jsou odesílány hraničním směrovačem oblasti, neboli ABR (Area Border Router), který těmito zprávami udává, jaké IPv6 prefixy patří do dané oblasti. Zprávy jsou generovány pro každý prefix zvlášť.
- **Inter-Area Router LSA:** Tyto LSA zprávy jsou ekvivalentem LSA zpráv typu 4 protokolu OSPFv2. Jsou vytvářeny ABR směrovačem a popisují cestu ke hraničnímu směrovači autonomního systému, neboli ASBR (Autonomous System Border Router), který propojuje autonomní systém protokolu OSPF s jiným systémem používajícím jiný směrovací protokol.
- **AS-External LSA:** Tyto LSA zprávy jsou ekvivalentem LSA zpráv typu 5 protokolu OSPFv2. Odesílá je ASBR a popisují cíle, které se nachází mimo lokální autonomní systém (AS). Mohou být využity k popisu výchozí cesty (default route).
- **Link LSA:** Jsou generovány směrovačem pro každou linku zvlášť. Jsou šířeny pouze na dané lince, ke které se vztahují. Nikdy se nešíří dál. Jejich účelem je informovat protější směrovač o „link-local“ adrese rozhraní směrovače a o IPv6 prefixech, které jsou asociovány s danou linkou.
- **Intra-Area Prefix LSA:** Směrovač využívá tyto zprávy, aby informoval ostatní směrovače, o připojených koncových oblastech k danému směrovači, o připojených tranzitních oblastech k danému směrovači, a které IPv6 prefixy jsou asociovány se směrovačem samotným.

[7]

LSA zprávy jsou tedy velice důležitým prvkem OSPFv3 protokolu, který je využívá k vzájemné komunikaci a výměně informací mezi jednotlivými směrovači.

[6][7][8]

1.4 Směrovací protokol IS-IS

Stejně jako u OSPF se jedná o dynamický směrovací protokol využívaný pro směrování uvnitř autonomních systémů, díky čemuž je označován jako IGP protokol. Rovněž patří do třídy *link-state* protokolů, které se při výpočtech nejkratších cest řídí stavy linek. IS-IS si vytváří databázi síťové topologie za pomoci Dijkstrova algoritmu pro výpočet nejkratších cest. Podle této databáze se pak rozhoduje, která cesta je tou nejkratší do cílové destinace. Dalšími společnými znaky mezi protokolem IS-IS a OSPF jsou:

- Využívají Hello zpráv pro navázání a udržování spojení s ostatními směrovači.
- Používají oblasti pro rozlišení sítě do dvouúrovňové hierarchie.

- Oba umožňují sumarizaci adres mezi oblastmi.
- Jedná se o CIDR protokoly (přeposílají informace o sítích včetně jejich masek – možnost vytvářet podsítě).
- Stanovení „designated“ směrovače v rozlehlých sítích.

Na rozdíl od OSPF, který byl vytvořen a standardizován organizací IETF, IS-IS byl vyvinutý společností DEC (Digital Equipment Corporation). Zprávy, které IS-IS používá pro rozesílání informací ostatním směrovačům v síti, se nazývají zkratkou LSP (Link-State Protocol data units). Tyto zprávy obsahují informace o IP cestách, kontrolních součtech apod.

1.4.1 Adresování

Ostatní směrovací protokoly běžně využívají TCP, UDP či IP protokoly, které operují na 3. nebo 4. vrstvě OSI modelu. IS-IS pracuje přímo na 2. vrstvě OSI modelu. Díky této skutečnosti, rozhraní, na kterých je v provozu směrovací protokol IS-IS, nepotřebují IP adresu. Identifikace v síti protokolu IS-IS probíhá pomocí adres zvaných Network Entity Titles (NET), volně přeloženo jako názvy síťových subjektů. Tyto adresy mohou být dlouhé 8 až 20 B, běžně se však používají v délce 10 B a jejich zápis vypadá následovně:

```
49.0001.1921.6800.1002.00
```

NET adresa se skládá z:

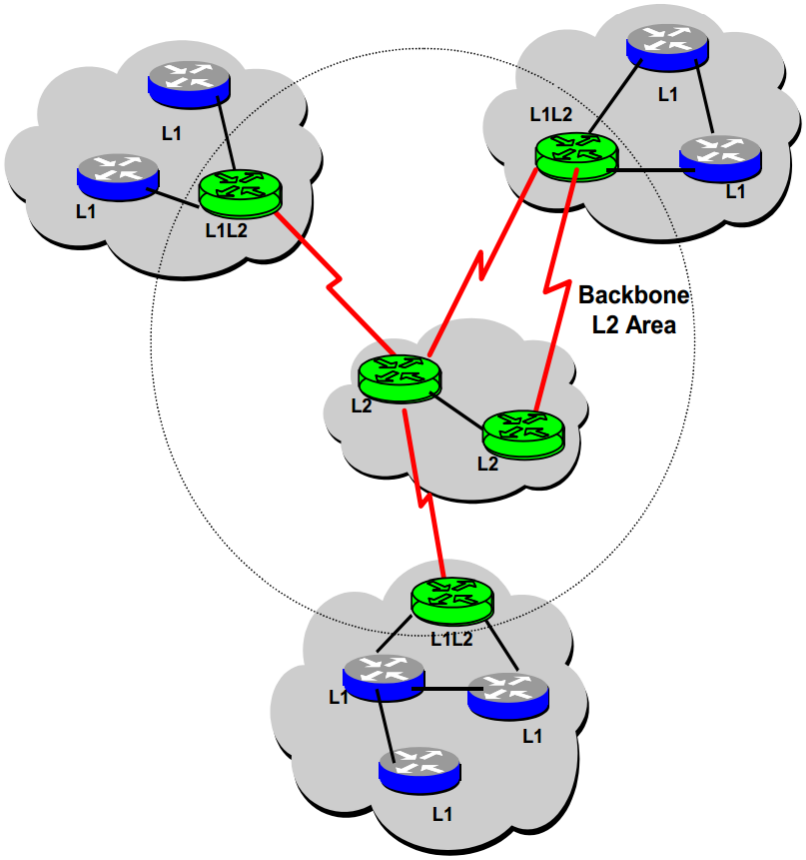
- **Identifikátor oblasti** – První tři bajty slouží k identifikaci oblasti. První bajt z předchozího příkladu – 49 – identifikuje adresní rodinu, která je ekvivalentní k IP adresnímu prostoru přiřazenému k autonomnímu systému.
  Zbylé dva bajty reprezentují ID oblasti, tudíž dle příkladu – 0001 – je ID oblasti číslo 1.
- **Identifikátor systému** – Dalších 6 bajtů slouží k identifikaci uzlu neboli směrovače v síti. Pro toto číslo si můžeme zvolit jakoukoliv hodnotu, nicméně jednou z běžných metod, jak získat tento identifikátor, je použitím IP adresy z rozhraní loopbacku, kterou doplníme o nuly, a po sléze rozdělíme tečkou do tří skupin po čtyřech číslicích.
  Př.: 192.168.1.2 > 192.168.001.002 > 1921.6800.1002
  Obdobnou metodou můžeme získat tento identifikátor z MAC adresy směrovače.
- **NET volič** – Poslední dva bajty musí být za použití IS-IS vždy nulové, indikují totiž „daný systém“.

[9]

1.4.2 Oblasti

Na rozdíl od protokolu OSPF, kde dochází k oddělování oblastí na hraničních směrovačích, u protokolu IS-IS k tomuto rozdělení dochází na lince mezi dvěma směrovači, které spojují dvě různé oblasti, z čehož vyplývá, že každý individuální směrovač náleží pouze jedné oblasti. Důvodem, proč je to řešeno zrovna tímto způsobem, je, že IS-IS směrovač má pouze jednu

NET adresu, přičemž směrovač v IP síti, má IP adresu jednu nebo více, což se odvíjí podle počtu využívaných rozhraní.



Obrázek 1.5: Příklad IS-IS sítě a její rozdělení do oblastí různých úrovní. [11]

IS-IS využívá dvouúrovňové hierarchie. Úroveň a použití určité oblasti je dáno úrovní směrovačů, které se v ní nachází.

- **Level 1** – směrovače první úrovně jsou využívány pro klasické směrování uvnitř oblasti, která náleží například poskytovateli internetu, či jiné korporaci. Směrovače L1 znají topologii pouze své vlastní oblasti, do které samy náleží. Sousedícími směrovači mohou být buď jiné L1 směrovače anebo směrovače typu L1/L2. Sestavují si databázi stavů linek pro úroveň L1 pomocí všech možných informací využitelných pro vnitřní směrování.
- **Level 2** – směrovače s označením druhé úrovně jsou považovány za „páteřní“ části sítě. L2 směrovač může mít sousedy ve stejné či jiné oblasti, sestavuje si databázi stavů linek druhé úrovně L2, ve které shromažďuje veškeré potřebné informace pro směrování mezi oblastmi. L2 směrovače znají všechny ostatní oblasti, včetně oblastí L1, nicméně již nemají přístup k L1 informacím, které si vyměňují směrovače mezi sebou ve své vlastní oblasti.
- **Level 1/2** – směrovače sloužící k propojení ostatních oblastí, či jednotlivých úrovní. L1/L2 směrovač může mít sousedy v jakékoliv oblasti, sestavuje si dvě databáze stavů

linek; L1 pro směrování uvnitř oblasti a L2 pro směrování vně mezi oblastmi. Díky této skutečnosti tyto směrovače operují se dvěma SPF procesy, to má však za následek větší nároky na operační paměť a procesor. Pokud je L1/L2 směrovač některou z jeho linek připojen do jiné oblasti, zaznamená to do svých LSP paketů. Kopii těchto LSP zpráv pak rozešle všem ostatním L1 směrovačům v jeho oblasti, ty pak vědí kam odesílat pakety, jejichž cílová adresa vede ven mimo svou vlastní oblast.

[10]

1.4.3 Podpora IPv6

Protokol IS-IS je postavený zcela jinak než jemu podobný směrovací protokol OSPF. Protokol OSPF dokáže provádět směrování pouze v sítích založených na protokolu IPv4, a pro podporu směrování v IPv6 sítích jej bylo nutné zcela přepsat, čímž vznikl protokol OSPFv3. Toto však u IS-IS není potřeba. Jelikož pro výměnu směrovacích informací nepoužívá IP adresy, nezáleží tak na typu adres přenášených za účelem směrování. Pro podporu IPv6 směrování bylo tak pouze přidáno a upraveno několik parametrů.

IS-IS používá TLV protokol, který specifikuje konkrétní parametry pro jednotlivé podporované protokoly, jejichž informace je schopen rozpoznat a nadále šířit pomocí IS-IS. Ke každému takovémuto protokolu existuje odpovídající hodnota v poli NLPID. Právě v tomto poli bylo nutné přidat hodnotu 0x81, která je nezbytná pro podporu IPv6 protokolu v IS-IS.

[12]

1.5 Směrovací protokol BGP4+

Na rozdíl od předešlých směrovacích protokolů je BGP4+ EGP (Exterior Gateway Protocol), tedy směrovací protokol využívaný především ke směrování mezi různými autonomními systémy (AS).

Každý AS má pro svou identifikaci uděleno číslo ASN (Autonomous System Number). ASN může být buďto veřejné nebo privátní. Veřejné ASN je přidělováno organizacemi RIR (Regional Internet Registry) nebo NIR (National Internet Registry). Pro privátní ASN je rezervován rozsah od AS64512 po AS65535 institucí IANA (Internet Assigned Numbers Authority). Organizace RIR je vždy zodpovědná za přidělování a správu IP adres a ASN pro konkrétní oblast na světě, příkladem je možno zmínit jedny z hlavních RIR: RIPE-NCC (Evropa), ARIN (Severní Amerika), AfriNIC (Afrika), apod. Na rozdíl od toho NIR je zodpovědná za přidělování a správu IP adres pro konkrétní stát.

BGP4+ se označuje jako „path-vector“ směrovací protokol. *Path-vector* je v podstatě posloupnost ASN, přes které vede cesta k cílové síti. Samotný princip tvoření *path-vector* záznamu je velice jednoduchý, každý hraniční směrovač daného AS, přes který cesta vede, zapíše číslo svého AS do *path-vector* záznamu, a přepošle jej dál. Ochrana před vznikem smyčky je zajištěna tak, že konkrétní ASN se může v *path-vector* záznamu objevit pouze jedenkrát. V případě, že směrovač najde své ASN v přijaté cestě, cestu zahodí.

Path-vector je rovněž využíván při volbě nejkratší cesty do cílové sítě, a to tak, že sečte kolika AS je potřeba na cestě k cílové síti projít. Cesta s nejmenším počtem AS je považována za nejkratší, taková bude později preferována při samotném výběru nejkratších cest.

[13][15]

1.5.1 Navazování spojení

BGP4+ pracuje pod protokolem TCP na portu 179. BGP4+ směrovač se označuje jako „BGP peer“ (dále jen „směrovač“). Jak již bylo zmíněno, jedná se o vnější směrovací protokol (EGP), nicméně velké organizace a firmy, které disponují stovkami poboček, využívají BGP4+ i pro směrování uvnitř AS. Z tohoto důvodu se rozlišuje vztah navázaného spojení mezi dvěma směrovači na vazbu *internal* BGP (IBGP) v rámci jednoho AS a *external* BGP (EBGP) mezi dvěma různými AS.

Vazba mezi dvěma směrovači začínání navázáním TCP spojení. Při navazování TCP spojení se může stát, že se oba směrovače pokusí započít TCP spojení mezi sebou ve stejný okamžik. Aby nedošlo k navázání dvou TCP spojení mezi dvěma směrovači, směrovač s menším BGP identifikátorem zruší svůj požadavek na vytvoření spojení. Jakmile je TCP spojení navázáno, dojde k výměně zpráv OPEN, načež následují zprávy KEEPALIVE, které potvrzují zprávy OPEN. V tomto bodě je vyjednávání spojení téměř u konce, a směrovače si již pouze vzájemně vymění směrovací databáze pomocí zpráv UPDATE. Popis zpráv vyměňovaných v průběhu sestavování spojení je popsán v následujícím odstavci.

- **OPEN** – Pomocí této zprávy se směrovače dohodnou například na verzi používaného protokolu BGP, předají si čísla svých AS a také délku časovače *Holdtime*.
- **KEEPALIVE –** Vyměňuje se v minutových intervalech a slouží k ověřování linky. Pokud po dobu *HoldTime* nedorazí od souseda zpráva KEEPALIVE, je spojení považováno za nefunkční. Takový případ je jedním z důvodů vyslání zprávy NOTIFICATION.
- **NOTIFICATION –** oznamuje chybu, po jejím odeslání se ukončí vazba mezi sousedními směrovači rozpojením TCP spojení.
- **UPDATE –** pomocí těchto zpráv se může šířit nová cesta, aktualizace již existující cesty, či požadavek na odstranění neplatné cesty. Směrovací informace jsou přenášeny ve formátu <prefix, délka prefixu>. Rozdíl mezi IPv4 a IPv6 protokolem nastává právě při odstraňování nefunkční cesty. U IPv4 se k výpisu cest, které mají být odstraněny, využívá pole s proměnnou délkou nazvané *Withdrawn Routes*, to specifikuje seznam neplatných cest. Pro IPv6 cesty se využívá atribut „MP_UNREACH_NLRI“, který obsahuje sekci *Withdrawn Routes* jež udává informaci o neplatných cestách v podobě prefixu sítě a jeho délky.

[13][15]

1.5.2 Atributy cest

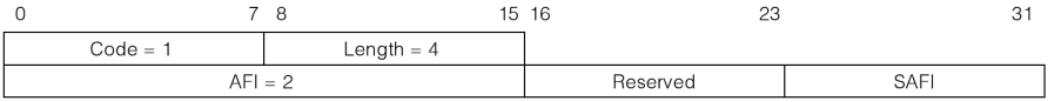
Atributy cest se využívají k popisu jejich různých vlastností. Právě těmito atributy můžeme ovlivnit směrovací politiku protokolu BGP4+. Můžeme určit, které AS budou tranzitní, které nikoliv apod. Z toho vyplývá, že algoritmus pro výběr cest s těmito atributy při výpočtu nejlepší cesty pracuje. Atributy se dělí do čtyř základních skupin:

- **Well-known mandatory** – musí je umět rozpoznat a zpracovat každý BGP směrovač. Tento typ atributů musí být obsažen v každé zprávě UPDATE, která obsahuje informace o dosažitelných cestách – NLRI (Network Layer Reachability Information).
- **Well-known discretionary** – rovněž je musí umět rozpoznat a zpracovat každý BGP směrovač. Tyto atributy nejsou povinné a mohou být ze zpráv UPDATE vypuštěny.
- **Optional transitive –** není vyžadováno, aby tyto atributy BGP směrovač podporoval. Tyto atributy nejsou povinné a mohou být ze zpráv UPDATE vypuštěny. V případě, že BGP směrovač dostane zprávu s takovými atributy a nerozumí jim, musí je přeposlat dalšímu BGP směrovači.
- **Optional non-transitive –** není vyžadováno, aby tyto atributy BGP směrovač podporoval. Tyto atributy nejsou povinné a mohou být ze zpráv UPDATE vypuštěny. V případě, že BGP směrovač dostane zprávu s takovými atributy a nerozumí jim, musí je ignorovat a dále již neposílat.

[14][15]

1.5.3 Podpora IPv6

BGP4+ směrovač, který dokáže pracovat s protokolem IPv6, musí tuto podporu dávat najevo správným nastavením parametrů způsobilosti ve zprávě OPEN. Obsažená pole zobrazující příslušné parametry jsou zobrazeny v obrázku 1.6.



Obrázek 1.6: Pole parametrů způsobilosti.[14]

První pole obsahuje kód, který je nastaven na číslo 1. To znamená podporu více-protokolových rozšíření. Dalším důležitým polem je AFI (Address Family Identifier), které je nastaveno na číslo 2. AFI je přidělováno institucí IANA a označuje používaný protokol síťové vrstvy (1 = IPv4, 2 = IPv6). Posledním polem je SAFI (Subsequent Address Family Identifier), které poskytuje dodatkové informace o přenášených NLRI.

Jsou definovány následující hodnoty:

- **1** – využíváno pro „unicast“
- **2** – využíváno pro „multicast“
- **3** – využíváno pro oba typy

Zprávy UPDATE, které nesou informace pouze o IPv6 sítích již neobsahují pole NLRI pro IPv4 cesty. Podobně i atribut NEXT_HOP, který má význam pouze pro IPv4 protokol, je možné vynechat ze zpráv, které nesou pouze informace o dosažitelných cestách v protokolu IPv6. V praxi se však tento atribut nastaví na hodnotu 0.0.0.0 a ve zprávách UPDATE, které nesou IPv6 NLRI je zahrnut. Hlavním důvodem proč se tento atribut stále používá, bylo zjištění, že některé implementace BGP odmítaly zprávy s chybějícím atributem NEXT_HOP, jelikož patří mezi atributy povinné.

[14][15]

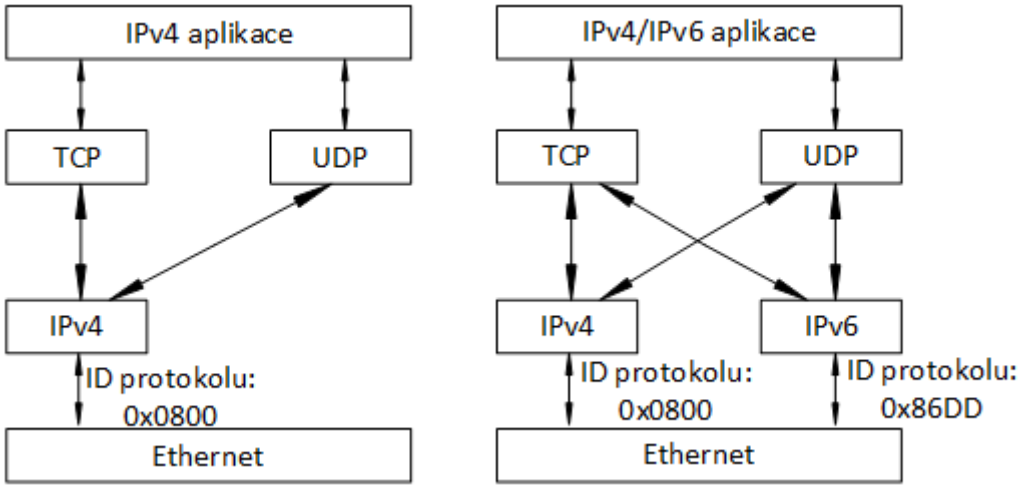
2 Koexistence zařízení pro IPv4 a IPv6

V současné době se stále více řeší protokol IPv6 a jeho využití v Internetu. Jedním z hlavních důvodů, proč se IPv6 protokol dostává do popředí, byl poměrně prudký nárůst počtu nejrůznějších chytrých zařízení (televize, domácí datová úložiště, osobní počítače, tablety či chytré telefony), která dnes běžně používáme a s nimi stále větší nedostatek IPv4 adres. Nahradit IPv4 protokol, a s ním veškerá systémová řešení, a další nejrůznější aplikace na něj navázané protokolem IPv6, nejde ze dne na den, a tudíž došlo ke vzniku několika různých mechanizmů, které nám umožňují provozovat oba zmíněné protokoly zároveň. Základní typy těchto mechanizmů a jejich konkrétní příklady jsou popsány v následující kapitole.

2.1 Technologie Dual Stack

Technologie Dual Stack je jedním z mechanizmů využívaných k přechodu z IPv4 sítě na síť IPv6. Síťové prvky podporující tuto technologii umožňují používat oba síťové protokoly zároveň. V praxi to znamená, že na jedné fyzické síti, běží v podstatě dvě logické topologie, jedna pod protokolem IPv4, druhá pod IPv6. Pokud však chceme mít plnohodnotnou síť, která podporuje oba protokoly zároveň, technologii Dual Stack musí podporovat všechna zařízení zapojená v této síti. Rozhraní jednotlivých prvků musí být nakonfigurována s IPv4 i IPv6 adresami.

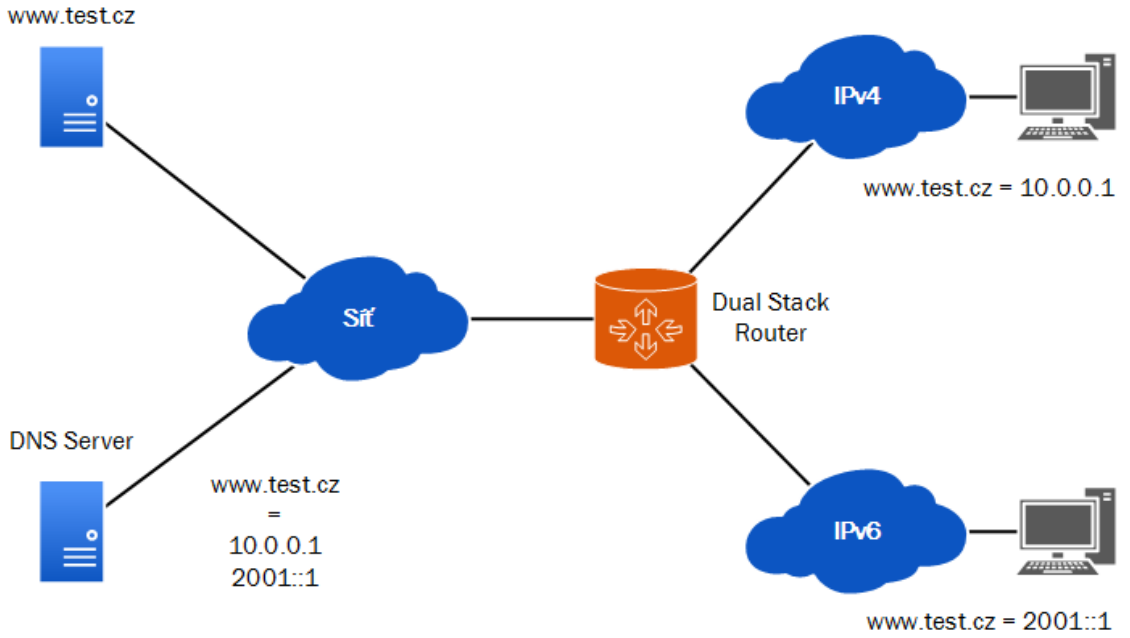
Obrázek 2.1 znázorňuje rozdíl Dual Stack řešení oproti klasickému použití pouze IPv4 protokolu. Ethernet je jedním z protokolů, který podporuje použití jak IPv4, tak novějšího IPv6 protokolu. Z toho důvodu bylo do hlavičky Ethernet rámce přidáno pole *Protocol ID*, které určuje, jaký paket dostane síťová vrstva. Pokud je hodnota ID rovna 0x0800, pak se jedná o IPv4 paket, pokud však 0x86DD, jedná se o IPv6.



Obrázek 2.1: Vlevo struktura použití pouze IPv4 protokolu, vpravo Dual Stack. [17]

Technologie Dual Stack je podporována několika protokoly pracujícími na aplikační vrstvě, jako je DNS, FTP, DHCP, Telnet a další. Na obrázku 2.2 je znázorněný příklad, jak taková síť využívající oba IP protokoly může fungovat. Klient ať už IPv4 sítě, či IPv6 sítě odešle

požadavek na DNS server, jakou IP adresu má doména www.test.cz. DNS server odpoví zprávou s požadovanou IP adresou, a to buď 10.0.0.1, nebo 2001::1. Pokud je požadavek od klienta na záznam typu A, dostane IPv4 adresu serveru test.cz, pokud je však na záznam AAAA, pak dostane v odpovědi IPv6 adresu daného serveru.



Obrázek 2.2: Typické využití sítě pracující s oběma protokoly – IPv4/IPv6.

2.2 Tunely

Technologie tunelů v síti pracuje na principu zapouzdření přenášených paketů. Tunel je v podstatě virtuální spojení typu bod-bod, které poskytuje cestu zapouzdřeným paketům. Zapouzdření probíhá na začátku tunelu, na jeho konci se pakety opět rozbalí. Tunel může být používán jednosměrně, či obousměrně, vše záleží na konfiguraci. Hlavním důvodem proč se tunely začaly používat, jsou takzvané „ostrovy“ IPv6 sítí uvnitř sítě většinového IPv4 protokolu. Proto vznikla potřeba tyto oddělené IPv6 sítě spojit – pomocí tunelů, které přenáší IPv6 pakety přes IPv4 síť. Aby byl tunel vytvořen, je potřeba určit začátek a konec. Z toho důvodu je nutné manuálně přiřadit IPv4 adresu na počátek tunelu. IPv4 adresa konce tunelu může být přiřazena manuálně nebo automaticky. Právě podle toho jakým způsobem je adresa konce tunelu přiřazena, rozlišujeme tunely na manuální a automatické.

2.2.1 Manuální tunely

Manuální tunely, také nazývány 6in4 tunely jsou ty, kterým musíme na začátek i konec ručně přidělit IPv4 adresu. Mezi tyto tunely se řadí také tunely typu Generic Routing Encapsulation, neboli GRE tunely, kde je celý IPv6 datagram zabalený uvnitř IPv4 paketu. Manuální tunely potřebují mít přidělenou také globální unicast IPv6 adresu, teprve pak jsou schopny přenášet data.

Obrázek 2.3 znázorňuje strukturu paketu, který prochází tunelem. Za IPv4 hlavičku, která obsahuje zdrojovou a cílovou IPv4 adresu je doplněna IPv6 hlavička následována datovou částí IPv6 paketu.

Obrázek 2.3: Struktura zapouzdřeného paketu, který je přenášen v tunelu. [16]

Naopak struktura paketu procházejícího přes GRE tunel obsahuje navíc ještě GRE hlavičku (viz. Obrázek 2.4).

Obrázek 2.4: Struktura zapouzdřeného paketu procházejícího přes GRE tunel. [17]

Mezi manuální typ tunelů patří technologie:

- IPv6 přes IPv4 manuální tunely
- IPv6 přes IPv4 GRE tunely

Prakticky ověřena byla konfigurace manuálního GRE tunelu na topologii sestavené ze zařízení Huawei i Cisco. Podrobné informace jak takovýto tunel nastavit, a jak funguje je obsaženo v kapitole 4. Praktické ověření koexistence zařízení pro IPv4 a IPv6.

2.2.2 Automatické tunely

Automatické tunely, označované taky jako dynamické tunely jsou ty, jejichž koncová adresa je doplněna automaticky. Výhodou tohoto typu tunelů je nejen možnost vytvářet spojení typu bod-bod, nýbrž i spojení typu bod-více bodů. Například 6to4 tunely využívají pro výpočet IPv6 adresy kombinaci 6to4 prefixu 2002::/16 a IPv4 adresy daného rozhraní hraničního směrovače (viz. Obrázek 2.5). Tím, že je cílová IPv4 adresa součástí cílové IPv6 adresy, je zařízení schopno tuto IPv4 adresu získat a doručit příslušný paket na odpovídající cílové rozhraní. Zapouzdření pak probíhá stejně jako u manuálních tunelů.

Obrázek 2.5: Prefix IPv6 adresy 6to4 tunelu, jeho délka činí 48bitů. [16]

Mezi automatické typy tunelů patří technologie:

- 6to4 tunely
- 6 Rapid Deployment
- ISATAP
- Teredo
- 6VPE
- NAT 64

[16][17]

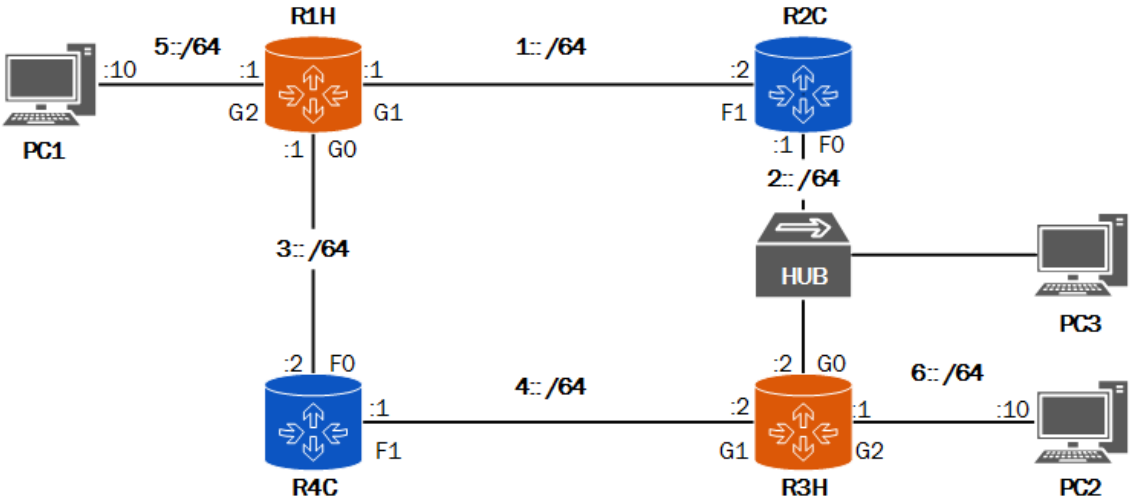
3 Praktické ověření směrovacích protokolů

Cílem této práce bylo ověřit funkci směrovacích protokolů pro IPv6 na zařízeních společnosti Huawei. K praktickému ověření byly využity prvky dostupné ve školní laboratoři. Jednalo se o tři směrovače, a to AR1220V, AR2220 a AR3260. Jelikož byly na laboratoři dostupné pouze tři prvky, v testovaných zapojeních byly doplněny o směrovače společnosti Cisco. Díky tomuto faktu byla zároveň s funkcí směrovacích protokolů ověřena i kompatibilita a vzájemná spolupráce mezi prvky těchto dvou výrobců.

Samotná konfigurace prvků byla prováděna za pomocí počítačů s operačním systémem Ubuntu a aplikace Minicom. Po patřičném nastavení a spojení sériového portu počítače s konzolovým portem prvku dojde k zobrazení rozhraní příkazové řádky ve zmíněné aplikaci. Po úspěšném propojení již konfigurujeme prvek textovými příkazy, které se odvíjí od výrobce a verze systému daného zařízení. K ověření správné funkčnosti zapojení bylo využito rozbočovače a ostatních počítačů s programem Wireshark, díky kterému je možno odchytávat komunikaci probíhající na připojené lince.

3.1 Směrování s pomocí RIPng

Pro svou jednoduchost implementace se směrovací protokol RIPng rozšířil především uvnitř malých sítí s nízkým počtem směrovačů. RIPng není příliš vhodný na implementaci do rozlehlých sítí, jelikož cesta může být dlouhá maximálně 15 skoků (resp. směrovačů), a velmi špatně odhaluje smyčky v topologii. V rozlehlých sítích není schopen odhalit směrovací smyčky téměř vůbec. Zde pak nastává problém zacyklení paketů a jejich zahazování. Hlubší teoretický rozbor naleznete v kapitole 1.2 Směrovací protokol RIPng. V následujícím odstavci je představena topologie, za pomocí které, byla testována funkcionalita směrovacího protokolu RIPng.



Obrázek 3.1: Topologie pro ověření směrovacího protokolu RIPng.

Testovaná topologie (viz. Obrázek 3.1) byla v konečném počtu složena ze čtyř směrovačů, jednoho rozbočovače pro odchytávání komunikace a třech počítačů, na kterých byla testována dostupnost a odchytáván provoz. Ke směrování byly využity dva prvky Huawei, konkrétně modely AR2220 a AR3260, a dva prvky Cisco, konkrétně modelová řada 2800. Směrovače Huawei jsou v topologii zobrazeny oranžovou barvou, směrovače Cisco barvou modrou. Prvky obou společností byly vzájemně promíchány tak, aby byla zaručena kompatibilita a ověření správné spolupráce. Jelikož je topologie zapojena do tvaru kruhu, vyskytuje se zde problém smyčky. Zároveň však nabízí více možností manipulace síťového provozu. Co je třeba na směrovačích Huawei nastavit, aby směrovací protokol RIPng fungoval správně, jaká další konfigurace byla použita k manipulaci provozu, a jaká další nastavení směrovacího protokolu byla provedena, je obsaženo v následující podkapitole 3.1.1 o konfiguraci prvků Huawei.

3.1.1 Konfigurace

Následující postup konfigurace se týká prvku R3H. Konfigurace ostatních zařízení Huawei je téměř analogická, mění se pouze čísla portů a nastavované IPv6 adresy. Konfigurace prvků Cisco se mírně liší svou syntaxí a konfiguračními příkazy, ukázková konfigurace alespoň jednoho prvku Cisco je zahrnuta v příloze A.

Jakmile je počítač připojen přes konzoli ke směrovači R3H, začneme následujícím příkazem:

```
<Huawei> system-view
```

Tímto se dostaneme do konfiguračního módu zařízení, odkud je možné upravovat aktuální konfiguraci prvku, včetně směrovacího protokolu RIPng. Že je zařízení v konfiguračním módu poznáme podle tvaru závorek, nyní už hranatých, svírajících jméno prvku.

```
[Huawei]
```

Jelikož se konfigurace více prvků najednou většinou provádí přes terminál jednoho počítače, např. připojením přes telnet, ssh nebo manuálním přepojením kabelu, je vhodné si prvky přejmenovat, abychom měli přehled, které prvky zrovna konfigurujeme. Proto směrovači změníme jméno Huawei na R3H dle schéma topologie.

```
[Huawei] sysname R3H
```

Jelikož budeme pracovat s IPv6 protokolem, je třeba ho povolit příkazem:

```
[R3H] ipv6
```

V této fázi již můžeme přejít ke konfiguraci rozhraní, která jsou v této topologii využívána. Užitečným příkazem, který nám zobrazí stručný přehled rozhraní prvku a jejich stav je:

```
[R3H] display ipv6 interface brief
```

Do konfigurace rozhraní přejdeme příkazem:

```
[R3H] interface GigabitEthernet0/0/0
```

Při běžné konfiguraci IPv4 protokolu stačí zadat IP adresu a rozhraní je připraveno přenášet pakety, nicméně u IPv6 protokolu je nejprve potřeba na každém rozhraní tento protokol povolit:

```
[R3H-GigabitEthernet0/0/0] ipv6 enable
```

Teprve nyní můžeme rozhraní zadat IPv6 adresu. Adresa se zadává ve formátu IPv6 adresy a délky prefixu odděleného mezerou viz. příkaz níže:

```
[R3H-GigabitEthernet0/0/0] ipv6 address 2::2 64
```

Stejným způsobem musíme povolit IPv6 protokol na všech zbývajících rozhraních, kde jej budeme využívat a stejně tak musíme na těchto rozhraních přidat i IPv6 adresu. To platí i pro ostatní prvky v síti. Pokud bychom adresu nepřidali, směrovače by se spolu domluvily, ale pouze na úrovni vztahů s přímými sousedy, tedy vždy ve dvojici na jedné lince. Tuto funkci podporuje samotný IPv6 protokol, a to pomocí tzv. Link-local adres. Link-local adresy vždy začínají prefixem FE80::/10 a jsou pouze lokálního významu dané linky, tudíž je nelze použít ke směrování, směrovače je využívají k nalezení sousedů a výměně základních informací.

Nyní můžeme přejít ke konfiguraci směrovacího protokolu RIPng. Proces směrovacího protokolu spustíme příkazem:

```
[R3H] ripng 1
```

Číslo 1 zde identifikuje konkrétní instanci směrovacího protokolu RIPng. Výše zmíněný příkaz nás přepne do její konfigurace, tu však v této fázi nepotřebujeme a proto použijeme příkaz pro opuštění konfigurace směrovacího protokolu.

```
[R3H-ripng-1] quit
```

Po zapnutí směrovacího protokolu na směrovači, je potřeba k dané instanci přiřadit i jednotlivá rozhraní, na kterých chceme provádět směrování. Zapnutí instance 1 protokolu RIPng na konkrétním rozhraní se provádí podobně jako aplikace IPv6 adresy na rozhraní. Vstoupíme do konfigurace daného rozhraní:

```
[R3H] interface GigabitEthernet0/0/0
```

A pak povolíme RIPng 1 příkazem:

```
[R3H-GigabitEthernet0/0/0] ripng 1 enable
```

Konfiguraci ukončíme příkazem:

```
[R3H-GigabitEthernet0/0/0] quit
```

Stejným postupem je nutné zapnout směrovací protokol RIPng i na ostatních směrovačích v síti. Konfigurace směrovačů Cisco se mírně liší, ukázku konfiguračního souboru zařízení Cisco,

konfigurační soubor zařízení Huawei pojmenovaného R3H a ostatní výpisy jsou obsaženy v příloze A.

3.1.2 Ověření funkčnosti

V této kapitole jsou obsaženy zejména příkazy a jejich výpisy, pomocí kterých je možné zkontrolovat správnou funkčnost protokolu a informace o topologii.

Zobrazit sousední směrovače, se kterými je navázána vazba přes protokol RIPng, je velmi užitečná funkce, kterou oceníme především v případech, kdy neznáme topologii sítě a máme k dispozici pouze přístup ke konfiguraci prvků.

```
[R3H] display ripng 1 neighbor
Neighbor: FE80::217:5AFF:FE4B:5821 GE0/0/1       Protocol: RIPNG
Neighbor: FE80::217:5AFF:FE4B:5358 GE0/0/0       Protocol: RIPNG
```

Z uvedeného výpisu je zřejmé, že směrovač R3H sousedí se dvěma směrovači, přes dvě fyzická rozhraní GigabitEthernet. Sousední směrovače jsou zde identifikovány pomocí link-local IPv6 adres (zmíněno v kapitole 3.1.1). Pokud si informace z tohoto výpisu srovnáme s obrázkem topologie (viz. Obrázek 3.1), zjistíme, že se v obou případech jedná o sousední směrovače Cisco.

Dalším užitečným příkazem je výpis databáze směrovacího procesu RIPng 1. Ten se nám zobrazí zadáním příkazu:

```
[R3H] display ripng 1 database
   1::/64, via FE80::217:5AFF:FE4B:5358, GE0/0/0, cost 1
   2::/64, GE 0/0/0, cost 0, RIPng-interface
   3::/64, via FE80::217:5AFF:FE4B:5821, GE 0/0/1, cost 1
   4::/64, GE 0/0/1, cost 0, RIPng-interface
   5::/64, via FE80::217:5AFF:FE4B:5358, GE 0/0/0, cost 2
   5::/64, via FE80::217:5AFF:FE4B:5821, GE 0/0/1, cost 2
   6::/64, GE 0/0/2, cost 0, RIPng-interface
```

Databáze obsahuje seznam všech dostupných sítí, které má směrovací protokol RIPng 1 k dispozici. Ve výpisu je uvedena link-local adresa sousedního prvku, přes který se k cílové síti dostaneme. RIPng si zde zapíše pouze nejkratší cestu k síti, resp. cestu s nejmenší metrikou. V případě sítě 5::/64, kdy existují do jedné sítě dvě různé cesty, si takové cesty směrovač v databázi ponechá. Všimněte si, že u přímo připojených sítí ke směrovači R3H je uvedena metrika cesty 0 a popisek RIPng-interface.

Nezbytnou a hojně využívanou funkcí je zobrazení směrovací tabulky konkrétního prvku. Typicky směrovače rozlišují směrovací tabulku pro protokol IPv4 a IPv6.

Z toho důvodu vypadá příkaz pro zařízení Huawei k zobrazení směrovací tabulky protokolu IPv6 následovně:

```
[R3H] display ipv6 routing-table

Routing Table : Public
        Destinations : 11       Routes : 12

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : FE80::217:5AFF:FE4B:5358     Preference   : 100
 Cost         : 1                            Protocol     : RIPng
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::                          PrefixLength : 64
 NextHop      : 2::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D
```

Směrovací tabulka obsahuje záznam pro každou cílovou síť, její prefix, délku prefixu, rozhraní a adresu příštího rozhraní na dané cestě do cílové sítě, prioritu cesty, metriku, protokol, za pomocí kterého, byl záznam ve směrovací tabulce vytvořen a doplňující informace. Jelikož je výpis směrovací tabulky poměrně zdlouhavý, jeho kompletní verze je obsažena v příloze A.

V neposlední řadě je také užitečný příkaz zobrazující souhrnné informace o konkrétní instanci protokolu RIPng.

```
[R3H] display ripng 1
Public vpn-instance
    RIPng process : 1
       Preference    : 100
       Checkzero     : Enabled
       Default-cost  : 0
       Maximum number of balanced paths : 8
       Update time   : 30 sec      Age time   : 180 sec
       Garbage-collect time : 120 sec
       Number of periodic updates sent : 651
       Number of trigger updates sent  : 34
       Number of routes in database    : 6
       Number of interfaces enabled    : 3
       Total number of routes : 4
       Total number of routes in ADV DB is : 7
```

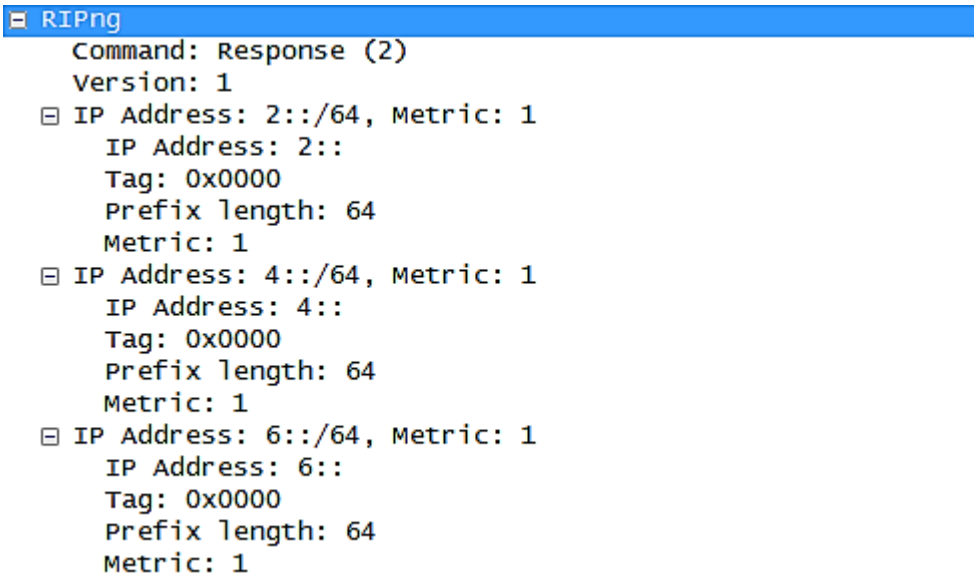
Výpis přehledně zobrazuje základní informace o nastavení instance 1 směrovacího protokolu RIPng. Hodnoty, které jsou zde vyobrazeny, jsou implicitní. Samozřejmě je lze upravovat pro potřeby směrování v konkrétní síti, např. hodnota pole *Preference* udává, jakou prioritu mají cesty získané od protokolu RIPng ve směrovací tabulce. Upravováním této hodnoty lze upřednostnit cesty jednoho směrovacího protokolu před jiným. Menší hodnota je brána jako větší priorita. Pole *Default-cost* určuje metriku pro cesty přejaté z jiných směrovacích protokolů, resp. externí cesty. Dále následuje série časovačů, jak často jsou zasílány aktualizace cest směrovacího protokolu, jak dlouho bude cesta obsažena ve směrovací tabulce, než bude prohlášena za neaktivní, a po jaké době bude cesta odstraněna úplně. Poslední částí tohoto výpisu jsou informace o aktuální topologii, počet aktuálně obsažených sítí ve směrovací tabulce, počet periodických aktualizací, počet vyvolaných aktualizací nějakou změnou ve směrovací tabulce na lokálním směrovači a počet rozhraní, na kterých je instance 1 protokolu RIPng aktivní.

Pro ověření konektivity byla spuštěna aplikace ping na počítači PC1 s cílem IPv6 adresy počítače PC2 (viz. Obrázek 3.2).

No.	Time	Source	Destination	Protocol	Info
4936	4940.103912	5::10	6::10	ICMPv6	Echo (ping) request id=0x0b42, seq=1906
4937	4940.104292	6::10	5::10	ICMPv6	Echo (ping) reply id=0x0b42, seq=1906

Obrázek 3.2: Pakety protokolu ICMPv6 zachycené programem Wireshark.

Na obrázku 3.3 je znázorněna zpráva – odpověď směrovače R3H na dotaz směrovače R2C protokolu RIPng. Zpráva zahrnuje lokální sítě směrovače R3H, tedy sítě přímo svázané s rozhraními směrovače. Informace obsažené ve zprávě přenáší prefix sítě, délku prefixu a metriku.



Obrázek 3.3: Zpráva protokolu RIPng obsahující informace o sítích.

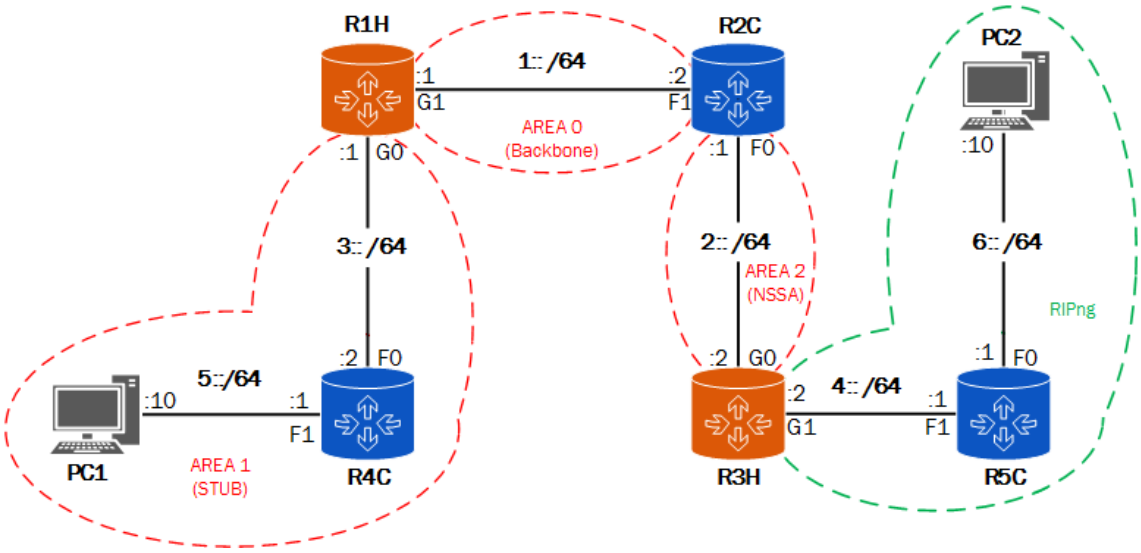
V podstatě se jedná o aktualizaci směrovací tabulky. Směrovač R2C si tyto informace porovná se svou směrovací tabulkou a v případě nalezených rozdílů si svou tabulku upraví, resp. aktualizuje.

3.2 Směrování s pomocí OSPFv3

Směrovací protokol OSPFv3 je hojně využívaný od středních po středně velké až rozlehlé sítě uvnitř korporací, školních kampusů apod. Jeho základní implementace je poměrně jednoduchá, zároveň však dovoluje široké možnosti nastavení chování směrovacího protokolu, rozdělení sítě na logické celky či rozložení zátěže způsobené směrováním. Hlubší teoretický rozbor naleznete v kapitole 1.3 Směrovací protokol OSPFv3.

Topologie k otestování funkce směrovacího protokolu OSPFv3 obsahuje 2 směrovače Huawei a 3 směrovače od společnosti Cisco, celkem tedy 5 směrovačů, které byly zapojeny a rozmístěny tak, aby byla ověřena i vzájemná spolupráce prvků mezi těmito výrobci. Dalšími zařízeními, které se v topologii objevily, byly dva počítače, pomocí kterých se testovala dostupnost a funkce sítě, rozbočovač a počítač s programem Wireshark, pro odchytávání komunikace probíhající mezi jednotlivými prvky. Topologie je rozdělena na několik oblastí, které jsou pro OSPF protokol tak typické. Hlavní, neboli páteřní oblastí je oblast označená popiskem AREA 0 (Backbone). K této oblasti musí být přímo připojeny všechny ostatní oblasti dané instance směrovacího protokolu OSPFv3. Z tohoto důvodu je oblast 0 umístěna uprostřed topologie a jsou k ní připojeny oblasti 1 a 2. Oblast 1 označená popiskem AREA 1 (STUB) je připojena k oblasti 0 přes směrovač R1H. Oblasti typu *stub* blokují veškeré LSA zprávy typu 5,

které přenáší informace o cestách do externích sítí, resp. do sítí, které byly do protokolu OSPFv3 redistribuovány z jiného směrovacího protokolu. Proto bychom ve směrovací tabulce prvku R4C marně hledali záznamy o sítích 4::/64 a 6::/64. Oblasti tohoto typu se považují za počáteční nebo konečné, objevují se tudíž na okraji sítě a provoz zde buď končí, nebo začíná. Třetí oblastí, která se v této topologii vyskytuje, nese číslo 2 a označení AREA 2 (NSSA). Tento typ oblasti – NSSA, je jediným, který dovoluje přenášet LSA zprávy typu 7. Tyto zprávy získáme redistribucí směrovacích informací z jiného směrovacího protokolu, z toho důvodu se v topologii vyskytuje část sítě běžící pod směrovacím protokolem RIPng.



Obrázek 3.4: Topologie pro testování OSPFv3.

Směrovač R3H zde plní funkci hraničního směrovače autonomního systému směrovacího protokolu OSPFv3, označuje se zkratkou ASBR (Autonomous System Boundary Router). Tento směrovač zajišťuje redistribuci směrovacích informací z externího směrovacího protokolu RIPng dovnitř autonomního systému směrovacího protokolu OSPFv3 a naopak. Takovéto směrovací informace jsou přenášeny právě LSA zprávami typu 7, které generuje ASBR a posílá je do oblasti 2 typu NSSA. Směrovač R2C v tomto případě plní funkci klasického hraničního směrovače uvnitř autonomního systému mezi oblastmi, neboli ABR (Area Border Router) a překládá LSA zprávy typu 7 na typ 5. Ty se již běžně šíří ostatními oblastmi mimo jakékoli *stub* oblasti, jak již bylo zmíněno v textu výše.

3.2.1 Konfigurace

Postup konfigurace v této podkapitole se vztahuje zejména na směrovače společnosti Huawei. Kompletní konfigurační soubory prvků jsou obsaženy v příloze B. Nejzajímavějším prvkem v této topologii je směrovač R3H, který byl záměrně umístěn tak, aby zároveň zajišťoval redistribuci směrovacích informací mezi oběma protokoly.

Prvním krokem při konfiguraci zařízení je nastavení jména, zapnutí podpory IPv6 protokolu jak globálně, tak i na jednotlivých rozhraních, a nastavení IPv6 adres. V tomto případě se jedná o rozhraní GE0/0/0 a GE0/0/1. Proto použijeme následující sérii příkazů:

```
[Huawei] sysname R3H
[R3H] ipv6
[R3H] interface GigabitEthernet0/0/0
[R3H-GigabitEthernet0/0/0] ipv6 enable
[R3H-GigabitEthernet0/0/0] ipv6 address 2::2/64
#
[R3H] interface GigabitEthernet0/0/1
[R3H-GigabitEthernet0/0/1] ipv6 enable
[R3H-GigabitEthernet0/0/1] ipv6 address 4::2/64
```

Podrobný postup s komentářem jak tato nastavení aplikovat je popsán v kapitole 3.1.1. Nyní přejdeme ke konfiguraci směrovacích protokolů a posléze k nastavení redistribuce směrovacích informací z jednoho směrovacího protokolu do druhého a naopak.

Nejdříve spustíme směrovací protokol OSPFv3.

```
[R3H] ospfv3
```

Tímto příkazem se zároveň dostaneme do konfigurace příslušné instance protokolu. Jelikož jsme číslo instance nespecifikovali při vytváření OSPFv3 procesu, je použito základní nastavení, které odpovídá instanci s číslem 1. V tomto kroku je potřeba nastavit identifikační číslo směrovače, které musí být jedinečné v rámci autonomního systému. Použijeme příkaz:

```
[R3H-ospfv3-1] router-id 3.3.3.3
```

Nyní vytvoříme oblast číslo 2 a nastavíme její typ na NSSA, aby zde mohlo docházet k redistribuci cest z jiného směrovacího protokolu.

```
[R3H-ospfv3-1] area 2
[R3H-ospfv3-1-area-0.0.0.2] nssa
```

Číslo oblasti a její typ by měl být na všech fyzicky připojených směrovačích do dané oblasti stejné, jinak nedojde k navázání sousedních vazeb směrovačů a směrování nebude fungovat. V této fázi zapneme protokol OSPFv3 na požadovaná rozhraní, v konkrétním případě se jedná pouze o jedno – GE0/0/0.

```
[R3H-GigabitEthernet0/0/0] ospfv3 1 area 0.0.0.2
```

Po zadání tohoto příkazu a správném nastavení ostatních směrovačů, které v topologii (viz. Obrázek 3.4) běží pod protokolem OSPFv3, bude směrování v této části sítě plně funkční. Nyní je potřeba nastavit směrovací protokol RIPng a po sléze vzájemnou redistribuci cest. Popis konfigurace protokolu RIPng již byl zmíněn dříve v kapitole 3.1.1, a proto zde nebude popsán postup krok po kroku. Protokol RIPng je potřeba zapnout a povolit na příslušném rozhraní – GE0/0/1. V této fázi jsou oba směrovací protokoly sice funkční, nedochází však k výměně informací mezi nimi, a tudíž směrování napříč celou topologií funkční není. Proto je potřeba

nastavit redistribuci cest z protokolu OSPFv3 do protokolu RIPng a naopak. Pokud by byla nastavena redistribuce cest pouze z jedné strany, pakety by se nedostaly zpět – neznaly by cestu.

Proto přejdeme do konfigurace protokolu OSPFv3:

```
[R3H] ospfv3
```

A zde zadáme sérii příkazů:

```
[R3H-ospfv3-1] default cost 25
[R3H-ospfv3-1] import-route ripng 1 type 2
```

Prvním příkazem nastavíme cenu externích cest pevně na 25. Každá cesta, která bude importována do protokolu OSPFv3 bude mít metriku 25. Druhým příkazem zajistíme již samotnou redistribuci z protokolu RIPng 1. Atribut *type* označuje způsob výpočtu metriky externí cesty. Typ 1 označuje, že metrika do dané externí sítě z libovolného OSPFv3 směrovače v testované topologii je rovna ceně cesty k ASBR (R3H) + cena externí cesty (25), zatímco typ 2 nic nesčítá, pouze zobrazuje metriku externí cesty (25) a to v každé části sítě, kam je informace o externí cestě šířena.

Pro protokol RIPng je potřeba nastavit cenu externích cest, a samotnou redistribuci z protokolu OSPFv3 instance 1. Nastavení typu metriky se u RIPng neprovádí.

```
[R3H] ripng 1
[R3H-ripng-1] default-cost 5
[R3H-ripng-1] import-route ospfv3 1
```

Konfigurace ostatních zařízení jsou obsaženy v příloze B.

3.2.2 Ověření funkčnosti

V této kapitole naleznete zejména příkazy a jejich výpisy, pomocí kterých je možné zkontrolovat správnou funkčnost protokolu a získat informace o topologii.

Užitečným příkazem je zobrazení základních informací o nastavení dané instance OSPFv3 protokolu. Výpis vyvoláme příkazem:

```
[R3H] display ospfv3 1
Routing Process "OSPFv3 (1)" with ID 3.3.3.3
 SPF Intelligent Timer[ms] Max: 10000, Start: 500, Hold: 2000
 LSA Intelligent Timer[ms] Max: 5000, Start: 500, Hold: 1000
 LSA Arrival interval 1000 ms
 Default ASE parameters: Metric: 25 Tag: 1 Type: 2
 Number of FULL neighbors 1
 Number of Exchange and Loading neighbors 0
```

```
 Number of LSA originated 5
 Number of LSA received 12
 Number of areas in this router is 1
```

Z výpisu zjistíme například důležité identifikační číslo směrovače, na kterém je příkaz spuštěn. Mezi další informace patří nastavení časovačů pro výpočet SPF algoritmu, zasílání LSA zpráv, počet odeslaných LSA zpráv, počet přijatých LSA zpráv, počet sousedů, se kterými je navázáno plně funkční spojení, počet sousedů, se kterými se spojení teprve vyjednává apod. Ve výpisu je rovněž zobrazen řádek *Default ASE parameters* (ASE = Autonomous System External), který zobrazuje nastavené parametry pro externí cesty, mezi kterými lze vidět, že základní metrika je nastavena na 25, jak bylo popsáno v konfiguraci. Na konci výpisu je rovněž důležitá informace o počtu oblastí, které jsou k tomuto směrovači vázány. U R3H se jedná pouze o jednu (viz. Obrázek 3.4 – topologie). Výpis je zkrácen a upraven tak, aby nezabíral příliš místa v textu, jeho kompletní verze je v příloze B.

Následující příkaz slouží k zobrazení informací o konkrétní oblasti, do které je přímo připojen směrovač R3H.

```
[R3H]display ospfv3 1 area
OSPFv3 Process (1)
  Area 0.0.0.2(NSSA)  Active
       Number of interfaces in this area is 1
       SPF algorithm executed 4 times
       Number of LSA 9.  Checksum Sum 0x2431c
       Number of Unknown LSA 0
```

Z výpisu je zřejmé, že se jedná o aktivní oblast 2 typu NSSA. Počet rozhraní směrovače R3H, které jsou do této oblasti zařazeny je 1.

Směrovací tabulka prvku R3H vypadá následovně:

```
[R3H]display ipv6 routing-table
 Destination  : 1::                          PrefixLength : 64
 NextHop      : FE80::217:5AFF:FE4B:5358     Preference   : 10
 Cost         : 2                            Protocol     : OSPFv3
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D
```

```
 Destination  : 2::                          PrefixLength : 64
 NextHop      : 2::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 6::                          PrefixLength : 64
 NextHop      : FE80::21E:F7FF:FEAC:4A63     Preference   : 100
 Cost         : 1                            Protocol     : RIPng
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1         Flags        : D
```

Tabulka není kompletní, byla upravena pro potřeby popisu v textu. Celá směrovací tabulka je obsažena v příloze B. Tento výpis obsahuje tři záznamy o sítích, kde každý z nich pochází z jiného „zdroje“. Informace o síti s adresou 1::/64 se ke směrovači dostala skrze směrovací protokol OSPFv3, cena cesty k této síti je 2. Další záznam popisuje síť 2::/64, která je přímo připojená na rozhraní směrovače R3H, a tudíž je u této sítě poznačen původ z protokolu „Direct“. Posledním záznamem je síť 6::/64, která je propagována směrovacím protokolem RIPng.

Nyní se podívejme, jak vypadá směrovací tabulka a nastavení OSPFv3 protokolu na směrovači R2C, který plní neméně důležitou funkci, a to překlad LSA zpráv typu 7 na typ 5.

Informace o konkrétní instanci směrovacího protokolu OSPFv3 zobrazíme příkazem:

```
R2C#show ipv6 ospf 1
```

Výsledkem je následující výpis:

```
 Routing Process "ospfv3 1" with ID 2.2.2.2
 Number of external LSA 2. Checksum Sum 0x00FC3F
 Number of areas in this router is 2. 1 normal 0 stub 1 nssa
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        SPF algorithm executed 13 times
        Number of LSA 9. Checksum Sum 0x042801
```

```
    Area 2
        Number of interfaces in this area is 1
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        SPF algorithm executed 18 times
        Number of LSA 11. Checksum Sum 0x0341E4
```

Je zřejmé, že směrovač R2C je na hranici mezi dvěma oblastmi – 0 a 2. Je tudíž považován za hraniční směrovač – ABR. Jelikož je na konci NSSA oblasti, LSA zprávy typu 7 musí překládat na zprávy typu 5, které se šíří v páteřní oblasti. Tato skutečnost je rovněž uvedena ve výpisu uvedeném výše.

Směrovací tabulka prvku R2C zobrazuje i záznamy o sítích přejatých z ostatních směrovacích protokolů, takové jsou v tabulce označeny zkratkou ON2 (OSPF NSSA ext 2), která označuje, že síť je externího původu z NSSA oblasti, a k výpočtu metriky byl použit typ 2.

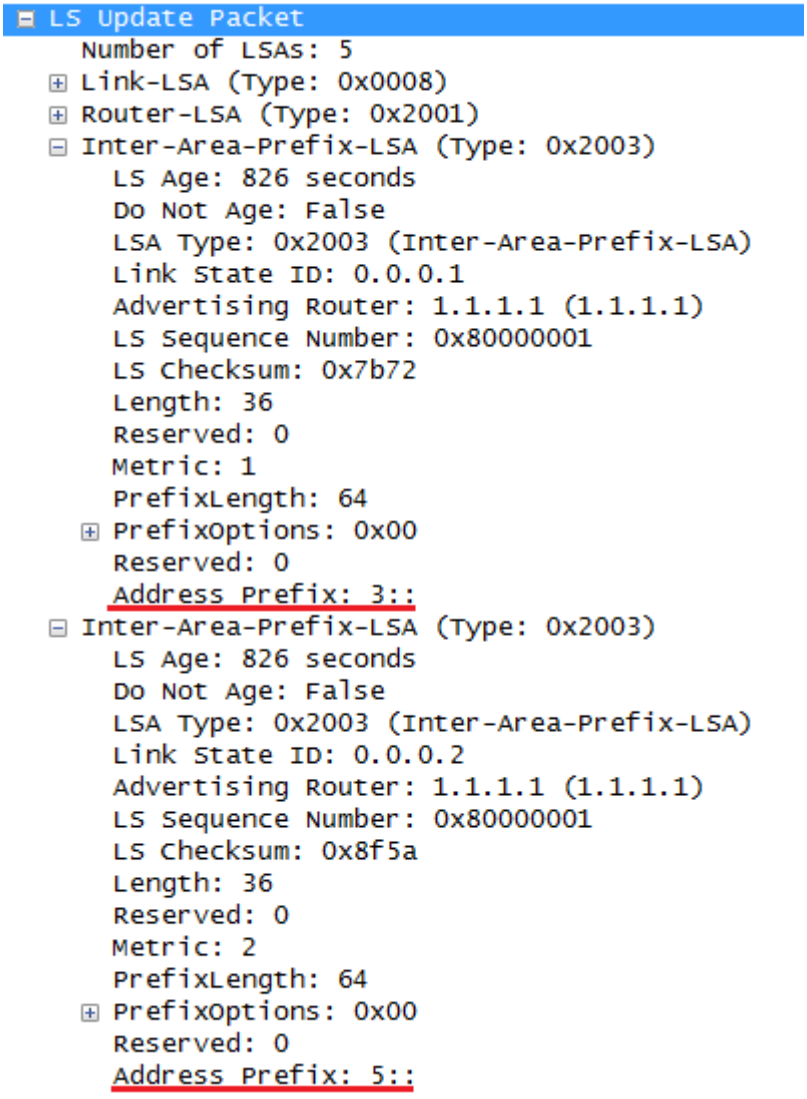
```
R2C#show ipv6 route
Codes: C - Connected, OI - OSPF Inter, ON2 - OSPF NSSA ext 2
C   1::/64 [0/0] via FastEthernet0/1, directly connected
C   2::/64 [0/0] via FastEthernet0/0, directly connected
OI  3::/64 [110/2] via FE80::A19:A6FF:FE9B:6D4F, FastEthernet0/1
ON2 4::/64 [110/25], tag 1 via FE80::A19:A6FF:FE9A:8276,FE0/0
OI  5::/64 [110/3] via FE80::A19:A6FF:FE9B:6D4F, FastEthernet0/1
ON2 6::/64 [110/25], tag 1 via FE80::A19:A6FF:FE9A:8276,FE0/0
```

Zcela jiná situace však nastává na prvku R4C, který je uvnitř oblasti 1 typu st*ub*. Do s*tub* oblastí se totiž nešíří LSA zprávy typu 5, které mají za úkol šířit informace o externích cestách. Z toho důvodu sítě 4::/64 a 6::/64 ve směrovací tabulce nenajdeme.

```
R4C#show ipv6 route
OI  1::/64 [110/2] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
OI  2::/64 [110/3] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
C   3::/64 [0/0] via FastEthernet0/0
C   5::/64 [0/0] via FastEthernet0/1
```

Na následujícím obrázku (Obrázek 3.5) je zobrazen zachycený paket LS Update, který přenáší informace o jednotlivých sítích v podobě LSA zpráv. Počet LSA zpráv obsažených v konkrétním LS Update paketu se odvíjí od počtu propagovaných cest či aktuálního stavu časovačů – tzn., že LS Update pakety jsou zasílány v různých časových intervalech s různým počtem LSA zpráv. Obrázek zachycuje LSA zprávy typu Link, Router a Inter-Area-Prefix, právě

poslední typ přenáší informace o síti dostupné uvnitř autonomního systému, konkrétně zde se jedná o sítě 3::/64 a 5::/64.



Obrázek 3.5: Zpráva LS Update zachycená v programu Wireshark.

LSA zprávy rovněž přenáší informaci, který směrovač zprávu odeslal, prefix šířené sítě, délku prefixu a především metriku do oněch sítí od původce dané zprávy.

Obrázek 3.6 již zobrazuje LSA zprávu typu 5, která šíří informace o externích cestách. Odeslal ji směrovač R2C, jedná se o síť s prefixem 4::/64, metrika do této sítě je 25, a způsob výpočtu metriky je nastaven na typ 2.

```
AS-External-LSA (Type: 0x4005)
    LS Age: 13 seconds
    Do Not Age: False
    LSA Type: 0x4005 (AS-External-LSA)
    Link State ID: 0.0.0.10
    Advertising Router: 2.2.2.2 (2.2.2.2)
    LS Sequence Number: 0x80000001
    LS Checksum: 0xcecc
    Length: 40
  Flags: 0x05 (E, T)
      .... .1.. = E: Type 2 external metric
      .... ..0. = F: Forwarding Address is NOT included
      .... ...1 = T: External Route Tag is included
    Metric: 25
    PrefixLength: 64
  PrefixOptions: 0x00
    Referenced LS type 0x0000 (Unknown)
    Address Prefix: 4::
    External Route Tag: 1
```

Obrázek 3.6: LSA zpráva typu 5.

LSA zpráva typu 7 může být vytvořena pouze ASBR směrovačem v oblasti typu NSSA. Taková zpráva je zobrazena na obrázku 3.7. Na směrovači R2C s identifikačním číslem 2.2.2.2 je přeložena na zprávu LSA typu 5 (viz. Obrázek 3.6).

```
LS Update Packet
    Number of LSAs: 1
  Type-LSA (Type: 0x2007)
      LS Age: 1 seconds
      Do Not Age: False
      LSA Type: 0x2007 (Type-LSA)
      Link State ID: 0.0.0.1
      Advertising Router: 3.3.3.3 (3.3.3.3)
      LS Sequence Number: 0x80000001
      LS Checksum: 0x05b5
      Length: 40
    Flags: 0x01 (T)
      Metric: 25
      PrefixLength: 64
    PrefixOptions: 0x08 (P)
      Referenced LS type 0x0000 (Unknown)
      Address Prefix: 4::
      External Route Tag: 1
```

Obrázek 3.7: LSA zpráva typu 7.

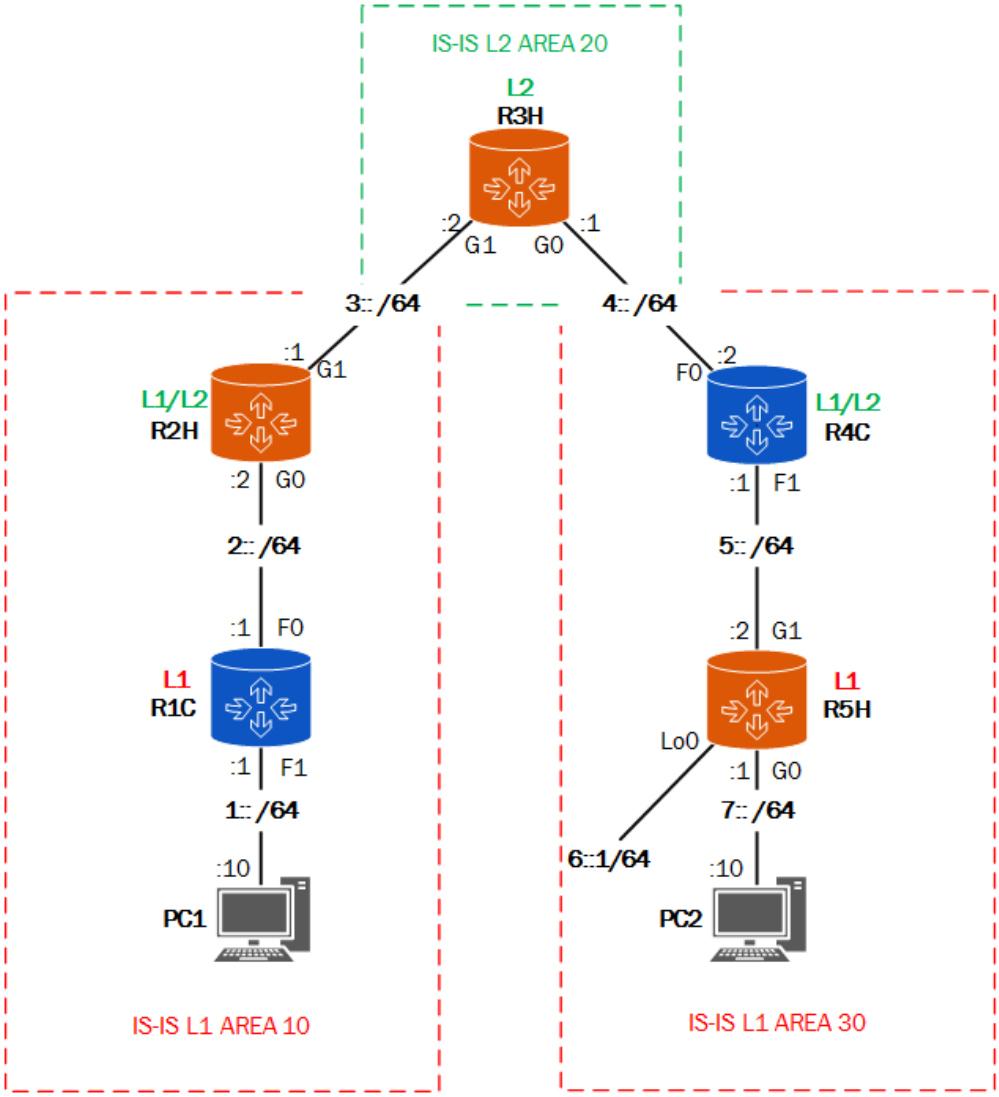
Konektivita byla ověřována v průběhu testování programem PING z lokálních počítačů. Obrázek 3.8 znázorňuje ověřování dostupnosti z PC1(5::10) na PC2(6::10).

No.	Time	Source	Destination	Protocol	Info
2238	476.385215	5::10	6::10	ICMPv6	Echo (ping) request id=0x0a02, seq=2512
2239	476.385801	6::10	5::10	ICMPv6	Echo (ping) reply id=0x0a02, seq=2512

Obrázek 3.8: Pakety protokolu ICMPv6 zachycené programem Wireshark.

3.3 Směrování s pomocí IS-IS

Směrovací protokol IS-IS je poměrně podobný protokolu OSPF. Nicméně pro svou univerzálnost je mnohdy využíván u složitějších sítí. Hodí se i pro velmi rozlehlé sítě, protože podporuje více směrovačů uvnitř jedné oblasti než jak je tomu u OSPF. Jelikož protokol IS-IS využívá data TLV, nebylo potřeba vyvíjet kompletně nový protokol kvůli podpoře IPv6 adres (OSPFv3). Podobností a odlišností mezi oběma protokoly je celá řada, to a jak protokol IS-IS funguje je popsáno v kapitole 1.4 Směrovací protokol IS-IS.



Obrázek 3.9: Topologie pro otestování IS-IS.

Topologie pro otestování IS-IS (Obrázek 3.9) obsahuje celkem tři oblasti. Dvě oblasti jsou typu L1, nesou označení IS-IS L1 AREA 10, IS-IS L1 AREA 30. Tyto oblasti se ve většině případech považují za „koncové“, tzn., že v takových to oblastech najdeme koncové sítě zákazníků. Nicméně není podmínkou, že by oblastmi typu L1 nemohl procházet tranzitní provoz, jako je tomu u protokolu OSPF a *stub* oblastí. U IS-IS je takovýto scénář povolen. Většinou jsou však oblasti L1 napojeny na oblast typu L2. Stejná varianta je zobrazena i na testovací topologii.

Zde se oblast 10 a 30 napojuje na oblast s označením IS-IS L2 AREA 20. Oblasti typu L2 jsou považovány za „páteřní“, a řídí provoz mezi jednotlivými L1 oblastmi. Tato hierarchie protokolu IS-IS dovoluje fyzickou síť rozdělit do logických celků, které pak nemusí být zatěžovány směrováním a směrovacími informacemi z celé rozlehlé sítě. Podrobnější rozbor testované topologie včetně výpisů ze směrovacích prvků je obsažen v kapitole 3.3.2 Ověření funkčnosti.

3.3.1 Konfigurace

Protokol IS-IS zapneme příkazem *isis* a číslem, které určuje konkrétní instanci protokolu:

```
[R5H] isis 1
```

Jakmile se dostaneme do konfigurace konkrétní instance směrovacího protokolu IS-IS, musíme nastavit úroveň, na které směrovač bude pracovat – L1 nebo L2, pokud úroveň ponecháme bez úprav, v základním nastavení je směrovač nastaven jako L1/L2 směrovač, který dokáže pracovat se směrovači obou úrovní.

```
[R5H-isis-1] is-level level-1
```

Dalším neméně důležitým úkonem v konfiguraci IS-IS protokolu je nastavení NET adresy, která jednak udává identifikátor oblasti, kam onen směrovač patří a identifikátor systému – adresu směrovače v rámci sítě IS-IS. Teorie k NET adresám a adresování ve směrovacím protokolu IS-IS je zpracovaná v kapitole 1.4.1 Adresování.

Adresu NET nastavíme příkazem:

```
[R5H-isis-1] network-entity 49.0030.5555.5555.5555.00
```

Posledním příkazem v řadě pro základní nastavení protokolu IS-IS je zapnutí podpory IPv6 protokolu.

```
[R5H-isis-1] ipv6 enable
```

Je-li nastaven a spuštěn směrovací protokol IS-IS, dalším krokem je povolit jej na jednotlivých rozhraních, jejichž sítě potřebujeme do sítě IS-IS propagovat. Takovéto rozhraní musí mít povolen protokol IPv6 a nastavenou IPv6 adresu. Protokol IS-IS povolíme na rozhraní příkazem:

```
[R5H-GigabitEthernet0/0/1] isis ipv6 enable 1
```

V tomto okamžiku bude protokol IS-IS bez problému funkční. Komunikace mezi směrovači však v základním nastavení není žádným způsobem šifrována či chráněna. Z toho důvodu bylo v topologii použito ověřování na úrovni jednotlivých rozhraní. Ověřování spustíme příkazem:

```
[R5H-GE0/0/1] isis authentication-mode simple plain Test
```

Tímto příkazem spustíme jednoduché ověřování na rozhraní G1 prvku R5H pomocí hesla Test. Toto heslo není nijak šifrováno díky atributu *plain* a lze jej bez problémů odchytit pomocí programu Wireshark (viz. Obrázek 3.10). Aby však ověřování fungovalo, musí být nastaveno

stejné heslo i na protějším konci týkající se linky. Dokud se tak nestane, směrovače budou vysílat pouze zprávy Hello a nedojde ke spojení a výměně směrovacích informací.

Směrovací protokol nabízí mimo autentifikace rozhraní i autentifikaci v rámci oblasti, či dokonce domény. Pro ukládání hesel může být využito jak prostého textu, tak i např. hašovací funkce MD5.

3.3.2 Ověření funkčnosti

V této kapitole naleznete zejména příkazy a jejich výpisy, pomocí kterých je možné zkontrolovat správnou funkčnost protokolu a informace o topologii.

V rámci oblasti L1 znají směrovače L1 pouze sítě, které se nachází ve stejné oblasti, za takové se považují i sítě, které jsou připojeny k L1/L2 směrovačům. Proto například směrovač R5H má ve své směrovací tabulce protokolu IS-IS celkem 4 sítě – 4::/64, 5::/64, 6::/64 a 7::/64.

```
[R5H]display isis route
                  Route information for ISIS(1)
                  ----------------------------
                 ISIS(1) Level-1 Forwarding Table
                 --------------------------------
 IPV6 Dest.  ExitInt     NextHop                   Cost   Flags
-------------------------------------------------------------------
 ::/0        GE0/0/1     FE80::217:5AFF:FE4B:5821  10     A/-/-
 4::/64      GE0/0/1     FE80::217:5AFF:FE4B:5821  20     A/-/-
 7::/64      GE0/0/0     Direct                    10     D/L/-
 6::/64      Loop0       Direct                    0      D/L/-
 5::/64      GE0/0/1     Direct                    10     D/L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-
IGP Shortcut, U-Up/Down Bit Set
```

Z uvedeného výpisu je zřejmé, že směrovač R5H nemá žádné informace o sítích nacházejících se mimo oblast 30.

Zcela jinak však vypadá směrovací tabulka na směrovači R4C, který jak je z testovací topologie zřejmé, je součástí stejné oblasti 30. Jelikož je směrovačem typu L1/L2, komunikuje a vyměňuje si směrovací informace jak s L1 sousedy – R5H, tak i s L2 sousedními směrovači – R3H. Z tohoto důvodu si udržuje směrovací tabulky dvě, jak pro L1 oblast 30, tak pro L2 oblast 20. Proto směrovací tabulka prvku R4C vypadá takto:

```
R4C#show ipv6 route
IPv6 Routing Table
Codes: C - Connected, L - Local, I1 - ISIS L1, I2 - ISIS L2, IA
- ISIS interarea, IS - ISIS summary
I2  1::/64 [115/40]   via FE80::A19:A6FF:FE9A:8276, FE0/0
I2  2::/64 [115/30]   via FE80::A19:A6FF:FE9A:8276, FE0/0
I2  3::/64 [115/20]   via FE80::A19:A6FF:FE9A:8276, FE0/0
C   4::/64 [0/0]   via ::, FE0/0
C   5::/64 [0/0]   via ::, FE0/1
I1  6::/64 [115/10]   via FE80::A19:A6FF:FE9B:B705, FE0/1
I1  7::/64 [115/20]   via FE80::A19:A6FF:FE9B:B705, FE0/1
```

Jelikož je R4C prvek společnosti Cisco, byl použit výpis kompletní směrovací tabulky prvku, nikoliv pouze směrovacího protokolu IS-IS. Proto je zde uveden pro srovnání i výpis prvku R2H společnosti Huawei, který je na stejné úrovni jako směrovač R4C, tedy L1/L2. Směrovač R2H se nachází v oblasti 10, proto bude mít ve své směrovací tabulce pro L1 pouze sítě z oblasti 10 – 1::/64, 2::/64 a síť s prefixem 3::/64, která propojuje oblast 10 typu L1 s oblastí 20 typu L2. Ve směrovací tabulce L2 bude směrovač obsahovat jak sítě k němu samotnému přímo připojené, tak i všechny ostatní sítě, které mu doručil směrovač typu L2 - R3H, nacházející se v oblasti 20. Proto směrovač typu L1/L2 hraje velmi důležitou roli pro svou konkrétní oblast. Ostatní směrovače L1 ze stejné oblasti si totiž k takovémuto směrovači pamatují cestu, kterou použijí v případě, kdy na nějaké z jejich rozhraní přijde paket s neznámou cílovou adresou, takový paket přepošlou na nejbližší L1/L2 směrovač, který má informace i o sítích mimo svou vlastní oblast. Jelikož L1/L2 směrovače provádí namísto jednoho rovnou 2 SPF výpočty, doporučuje se, aby tyto směrovače měly výkonnější hardware, obzvlášť ve velkých sítích.

```
[R2H]display isis route
                  Route information for ISIS(1)
                  ----------------------------
                 ISIS(1) Level-1 Forwarding Table
                 --------------------------------
 IPV6 Dest.  ExitInt     NextHop                     Cost   Flags
-------------------------------------------------------------------
 3::/64      GE0/0/1     Direct                      10     D/L/-
 2::/64      GE0/0/0     Direct                      10     D/L/-
 1::/64      GE0/0/0     FE80::217:5AFF:FE4B:5358    20     A/L/-
```

```
                ISIS(1) Level-2 Forwarding Table
                --------------------------------

 IPV6 Dest.  ExitInt     NextHop                    Cost   Flags
-------------------------------------------------------------------
 4::/64      GE0/0/1     FE80::A19:A6FF:FE9A:8277   20     A/-/-
 3::/64      GE0/0/1     Direct                     10     D/L/-
 7::/64      GE0/0/1     FE80::A19:A6FF:FE9A:8277   40     A/-/-
 2::/64      GE0/0/0     Direct                     10     D/L/-
 6::/64      GE0/0/1     FE80::A19:A6FF:FE9A:8277   30     A/-/-
 5::/64      GE0/0/1     FE80::A19:A6FF:FE9A:8277   30     A/-/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-
IGP Shortcut, U-Up/Down Bit Set
```

Mimo výpisy směrovacích tabulek, je rovněž velmi užitečné znát sousední směrovače, se kterými jsou navázány sousední vazby. K vypsání sousedních směrovačů použijeme příkaz:

```
[R2H]display isis peer

                  Peer information for ISIS(1)

System Id      Int     Circuit Id        State HoldTime Type PRI
------------------------------------------------------------------
1111.1111.1111 GE0/0/0 2222.2222.2222.01 Up    23s      L1   64
3333.3333.3333 GE0/0/1 2222.2222.2222.02 Up    30s      L2   64

Total Peer(s): 2
```

Z uvedeného výpisu vyplývá, že směrovač R2H sousedí se dvěma dalšíma směrovači, a to R1C, jehož ID tvoří samé jedničky, vazba je navázána přes fyzické rozhraní GE0/0/0 a jedná se o typ L1. Naopak vazba se směrovačem R3H je typu L2. Kolonka *Circuit Id* identifikuje IS-IS rozhraní, na kterém je tato vazba navázána. Identifikace IS-IS rozhraní je tvořena identifikátorem systému a pořadovým číslem rozhraní.

Součástí testování směrovacího protokolu IS-IS nebyla pouze základní schopnost směrování, nýbrž i základní úroveň zabezpečení na úrovni rozhraní. Zabezpečení rozhraní funguje na základě hesla/klíče, které je potřeba nastavit na obou stranách linky, pokud se hesla shodují, směrovače na dané lince navážou spojení a začnou si vyměňovat LSP zprávy. Pokud se

hesla neshodují, oba směrovače si posílají pouze zprávy Hello (viz. Obrázek 3.10), které zahrnují pouze základní informace o daném systému a jeho nastavení.

```
ISIS HELLO
    Circuit type             : Level 1 and 2, reserved(0x00 == 0)
    System-ID {Sender of PDU} : 2222.2222.2222
    Holding timer: 30
    PDU length: 1497
    Priority                 : 64, reserved(0x00 == 0)
    System-ID {Designated IS} : 2222.2222.2222.02
  Area address(es) (4)
      Area address (3): 49.0010
  IS Neighbor(s) (6)
      IS Neighbor: HuaweiTe_9a:82:77
  IPv6 Interface address(es) (16)
      IPv6 interface address: fe80::a19:a6ff:fe9b:6d4f (fe80::a19:a6ff:fe9b:6d4f)
  Protocols Supported (1)
      NLPID(s): IPv6 (0x8e)
  Authentication (5)
      clear text (1), password (length 4) = Test
```

Obrázek 3.10: Zpráva HELLO protokolu IS-IS zobrazující heslo používané k autentifikaci.

Mezi tyto informace patří typ vazby, jakou je možné navázat, identifikační číslo systému odesílatele, adresu oblasti, název souseda, IPv6 adresu rozhraní, jaké protokoly jsou podporovány, v případě zapnuté autentifikace je zde i záložka pro ověřování, která obsahuje samotné heslo. Toto heslo není v tomto konkrétním případě šifrováno, a je uloženo ve formě obyčejného textu.

```
ISO 10589 ISIS Link State Protocol Data Unit
  PDU length: 129
  Remaining lifetime: 1199
  LSP-ID: 3333.3333.3333.00-00
  Sequence number: 0x00000011
  Checksum: 0xe47d [correct]
  Type block(0x03): Partition Repair:0, Attached bits:0, Overload bit:0, IS type:3
    0... .... = Partition Repair: Not supported
    .000 0... = Attachment: 0
    .... .0.. = Overload bit: Not set
    .... ..11 = Type of Intermediate System: Level 2 (3)
  Protocols supported (1)
    NLPID(s): IPv6 (0x8e)
  Multi Topology (2)
  Area address(es) (4)
    Area address (3): 49.0020
  IS Reachability (23)
    Reserved value 0x00, must == 0
    IS Neighbor:  3333.3333.3333.02
    IS Neighbor:  2222.2222.2222.02
  IPv6 Interface address(es) (32)
    IPv6 interface address: 4::1 (4::1)
    IPv6 interface address: 3::2 (3::2)
  IPv6 reachability (28)
    IPv6 prefix: 4::/64, Metric: 10, Distribution: up, internal, no sub-TLVs present
      IPv6 prefix: 4::/64
      Metric: 10
      Distribution: up, internal
      no sub-TLVs present
    IPv6 prefix: 3::/64, Metric: 10, Distribution: up, internal, no sub-TLVs present
      IPv6 prefix: 3::/64
      Metric: 10
      Distribution: up, internal
      no sub-TLVs present
```

Obrázek 3.11: Zpráva LSP typu L2 protokolu IS-IS odchycená programem Wireshark.

LSP zprávy jsou zodpovědné za šíření směrovacích informací napříč topologie IS-IS protokolu. Z obrázku 3.11 můžeme zjistit, že tato konkrétní zpráva byla odeslána ze směrovače R3H, který pracuje na úrovni L2 a náleží do oblasti 20. Nejdůležitější jsou však propagované informace o sítích – 3::/64 a 4::/64, do kterých má směrovač R3H metriku 10.

Konektivita spojení byla ověřována v průběhu testování programem PING z lokálních počítačů. Obrázek 3.12 znázorňuje zachycené pakety programem Wireshark z PC1(1::10) na PC2(7::10).

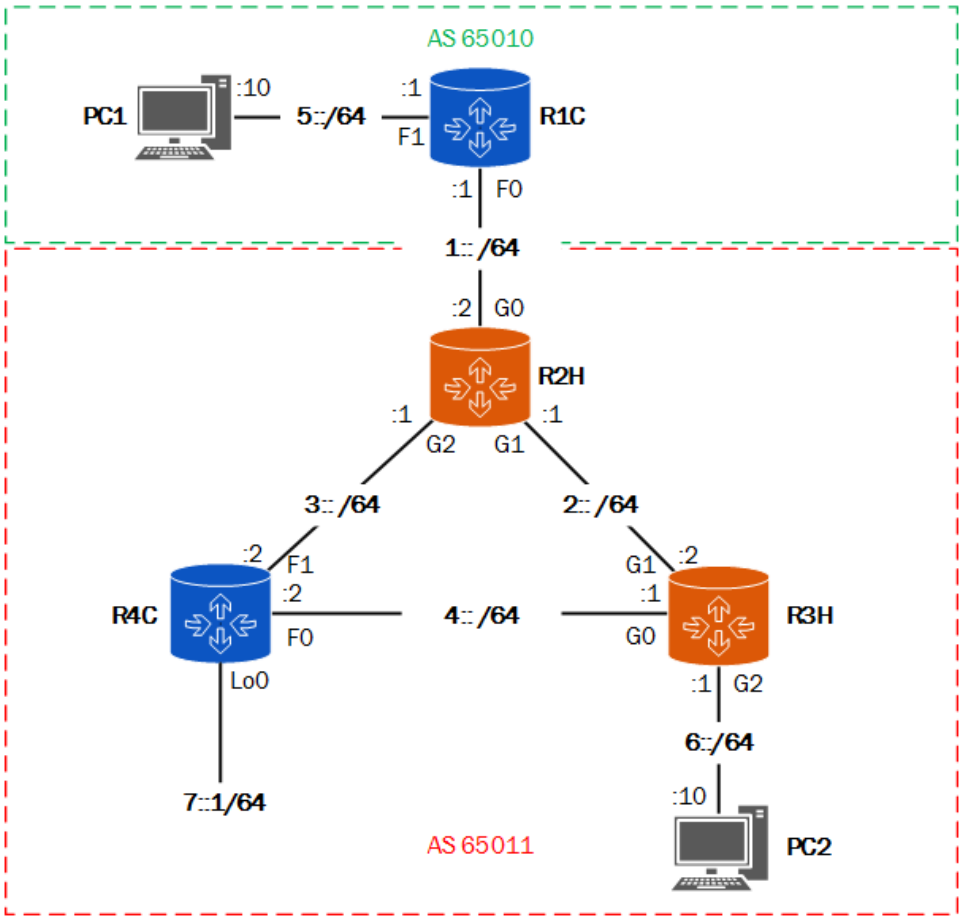
No.	Time	Source	Destination	Protocol	Info
2927	1158.404634	7::10	1::10	ICMPv6	Echo (ping) reply id=0x0a7a, seq=142
2929	1159.405338	1::10	7::10	ICMPv6	Echo (ping) request id=0x0a7a, seq=143

Obrázek 3.12: Pakety protokolu ICMPv6 zachycené programem Wireshark.

Doplňující výpisy z použitých zařízení, konfigurační výpisy apod. jsou obsaženy v příloze C.

3.4 Směrování s pomocí BGP4+

Směrovací protokol BGP4+ se poměrně razantně liší od předešlých protokolů v tom, kde se daný protokol využívá.



Obrázek 3.13: Topologie pro otestování protokolu BGP4+.

BGP4+ patří do kategorie externích směrovacích protokolů a jeho úkolem je směrovat mezi jednotlivými AS, nikoliv uvnitř, jak tomu bylo u předešlých testovaných protokolů. Díky tomuto faktu, je protokol BGP4+ využíván především poskytovateli služeb internetu ve velkých a rozlehlých sítích, či v sítích páteřních. Konfigurace směrovacího protokolu BGP4+ je poněkud více manuální, než u protokolů předchozích, jednotlivé vazby mezi směrovači je potřeba nastavit „ručně“ pomocí několika příkazů, stejně jako propagované sítě apod. Bližší teoretický rozbor je obsažen v kapitole 1.5 Směrovací protokol BGP4+.

Topologie (Obrázek 3.13) pro otestování směrovacího protokolu BGP4+ je sestavena ze 4 směrovačů a dvou počítačů. Síť je rozdělena do dvou autonomních systémů, aby byla otestována jak interní IBGP vazba, jejímž úkolem je výměna informací se sousedními směrovači uvnitř jednoho AS, tak externí EBGP vazba, která zaručuje výměnu směrovacích informací mezi různými AS. Směrovače Huawei a Cisco byly v topologii umístěny tak, aby se ověřila jejich vzájemná spolupráce.

3.4.1 Konfigurace

Prvním krokem je provedení základní konfigurace všech prvků v síti, tj. nastavení jmen směrovačů, zapnutí podpory směrování s IPv6, nastavení IPv6 adres na všech používaných rozhraních, apod. Jak nastavit tyto základní věci je krok po kroku popsáno v kapitole 3.1.1 Konfigurace. Z toho důvodu zde nebudou tyto základní příkazy znova popisovány, a rovnou přejdeme ke konfiguraci protokolu BGP4+.

Směrovací protokol BGP4+ spustíme následujícím příkazem, ve kterém musíme zároveň určit číslo autonomního systému, do kterého daný směrovač náleží. V případě směrovače R2H se jedná o AS s číslem 65011.

```
[R2H] bgp 65011
```

Stejně jako u většiny ostatních směrovacích protokolů, i u BGP je potřeba nastavit identifikační číslo směrovače. Příkaz je v podstatě stejný jako u směrovacího protokolu OSPFv3.

```
[R2H-bgp] router-id 2.2.2.2
```

Nyní je potřeba nastavit, resp. navázat BGP vazby se sousedními směrovači. Jak již bylo zmíněno v úvodním textu této kapitoly, protokol BGP rozlišuje vazby podle čísel AS na externí (mezi dvěma AS) a na interní (uvnitř jednoho AS). Proto je nutné při zadávání následujících příkazů dbát na správné přiřazení adresy rozhraní směrovače k AS, kam směrovač patří. Na konkrétním směrovači R2H proto nastavíme vazbu externí se směrovačem R1C (1::1), a vazby interní se směrovači R3H (2::2) a R4C (3::2).

```
[R2H-bgp] peer 1::1 as-number 65010
[R2H-bgp] peer 2::2 as-number 65011
[R2H-bgp] peer 3::2 as-number 65011
```

Výběr vazby nevolíme přímo konkrétním příkazem, směrovač sám porovná číslo svého AS s těmi, které zadáme u jednotlivých sousedů, a pokud jsou tyto ASN stejné, zvolí IBGP vazbu,

pokud se liší, tak naváže EBGP vazbu. Dalším příkazem umožníme konfiguraci BGP protokolu přímo pro IPv6 protokol, která je v této fázi nezbytná pro povolení přidaných sousedních směrovačů předchozími příkazy, a pro zadání IPv6 prefixů, které bude směrovač šířit.

```
[R2H-bgp] ipv6-family unicast
[R2H-bgp-af-ipv6] peer 1::1 enable
[R2H-bgp-af-ipv6] peer 2::2 enable
[R2H-bgp-af-ipv6] peer 3::2 enable
[R2H-bgp-af-ipv6] network 1:: 64
[R2H-bgp-af-ipv6] network 2:: 64
[R2H-bgp-af-ipv6] network 3:: 64
```

Povolili jsme navázání vazeb se všemi třemi sousedními směrovači, včetně všech třech sítí, které se budou pomocí protokolu BGP4+ šířit.

Konfigurace na směrovačích společnosti Cisco je velmi podobná, nicméně je potřeba zadat jeden příkaz navíc, který se u prvků Huawei neaplikuje. Například konfigurace směrovacího protokolu BGP4+ na prvku R1C vypadá následovně:

```
router bgp 65010
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 neighbor 1::2 remote-as 65011
 !
 address-family ipv6
  neighbor 1::2 activate
  network 1::/64
  network 5::/64
 exit-address-family
!
```

Příkazem tzv. „navíc“ je právě *no bgp default ipv4-unicast,* který ruší základní nastavení, že protokol BGP bude pracovat s adresní rodinou IPv4. Tento příkaz je potřeba zadat ještě před přidáváním vazeb na sousední směrovače.

3.4.2 Ověření funkčnosti

V této kapitole naleznete zejména příkazy a jejich výpisy, pomocí kterých je možné zkontrolovat správnou funkčnost protokolu a informace o topologii.

Základním prvkem směrovacího protokolu BGP jsou již zmiňované BGP vazby mezi jednotlivými směrovači. Následujícím příkazem zobrazíme vazby a jejich stav na prvku R2H.

```
[R2H]display bgp ipv6 peer


 BGP local router ID : 2.2.2.2
 Local AS number : 65011
 Total number of peers : 3        Peers in established state : 3

Peer V    AS  MsgRcvd MsgSent OutQ  Up/Down        State PrefRcv
1::1 4 65010       45      58    0 00:42:36  Established       2
2::2 4 65011       77      88    0 01:12:45  Established       3
3::2 4 65011        5       6    0 00:00:10  Established       3
```

Uvedený výpis udává identifikační číslo (2.2.2.2) lokálního směrovače, které odpovídá prvku R2H. Rovněž oznamuje, že číslo lokálního AS, resp. autonomního systému, ve kterém se směrovač nachází, je 65011. Celkový počet sousedních směrovačů je 3, z toho jsou všechny tři spojení úspěšně navázána. V tabulce jsou pak shrnuty podrobnější informace o každé vazbě, jako IPv6 adresa souseda, verze BGP protokolu, ASN, počet přijatých a odeslaných zpráv, počet zpráv k odeslání, doba, po kterou se nachází v daném stavu a počet prefixů přijatých od daného souseda.

Dalším příkazem nezbytným ke kontrole správné funkce směrování je vypsání směrovací tabulky prvku.

```
[R2H]display ipv6 routing-table


 Destination  : 4::                        PrefixLength : 64
 NextHop      : 2::2                       Preference   : 255
 Cost         : 0                          Protocol     : IBGP
 RelayNextHop : ::                         TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1       Flags        : RD

 Destination  : 5::                        PrefixLength : 64
 NextHop      : 1::1                       Preference   : 255
 Cost         : 0                          Protocol     : EBGP
 RelayNextHop : ::                         TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0       Flags        : D
```

```
 Destination  : 7::                          PrefixLength : 64
 NextHop      : 3::2                        Preference   : 255
 Cost         : 0                           Protocol     : IBGP
 RelayNextHop : ::                          TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/2        Flags        : RD
```

Směrovací tabulka uvedená výše, je zkrácená pro svou přílišnou délku a také z důvodu lepší přehlednosti. Kompletní směrovací tabulka je obsažena v příloze D. Zkrácená směrovací tabulka tedy obsahuje celkem tři sítě – síť 4::/64, která přišla od směrovače R3H z jeho rozhraní s adresou 2::2 na rozhraní GE0/0/1 prvku R2H. Jako protokol, přes který byla informace o této síti doručena, je udán IBGP, jelikož směrovač R3H patří do stejného AS s číslem 65011 jako směrovač R2H. U záznamu sítě 5::/64 je uveden protokol EBGP, jelikož informace o této síti pochází od směrovače R1C, který leží v AS s číslem 65010. Síť 7::/64 je ve směrovací tabulce uvedena z důvodu demonstrace principu funkce IBGP vazeb.

U externího BGP protokolu je vzniku smyček zamezeno tím, že AS nepřijme ty cesty, které ve svém *path-vector* již obsahují jeho číslo. Uvnitř AS, kde pracuje interní BGP protokol, však tato metoda použít nelze. Proto jsou definovány následující dodatečné podmínky pro šíření směrovacích informací uvnitř AS:

- Informace přijatá z IBGP se šíří na EBGP sousedy, nešíří se však na IBGP sousedy.
- Informace přijatá z EBGP se šíří na všechny ostatní EBGP i IBGP sousedy.

[15]

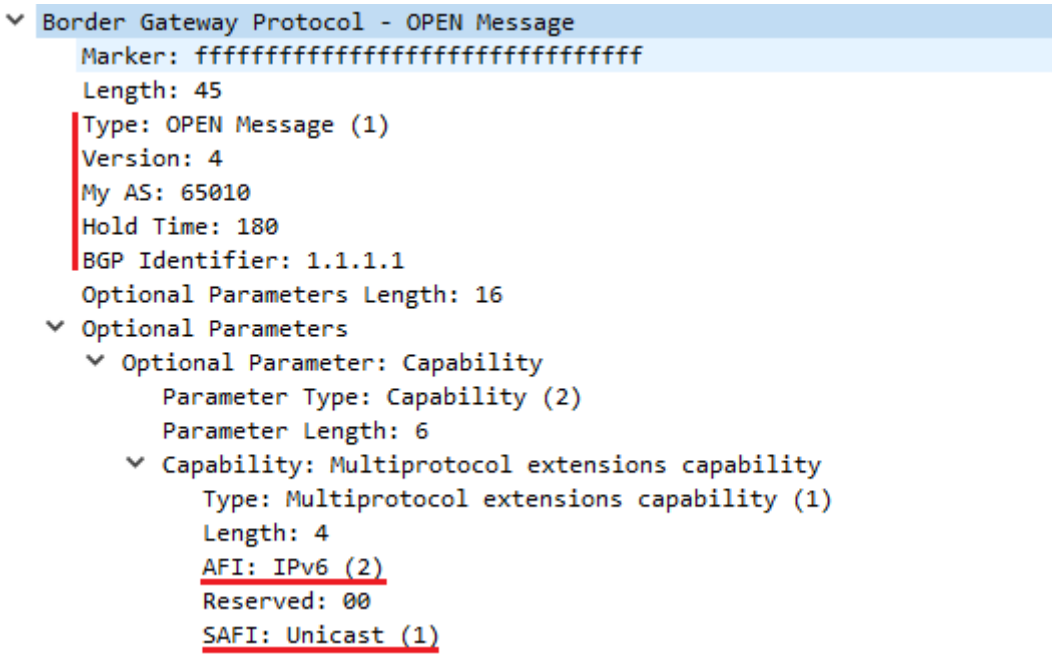
Právě díky těmto pravidlům, musí být IBGP směrovače zapojeny v tzv. „full mesh“ topologii. Pokud by tak nebylo učiněno i v testované topologii (Obrázek 3.13), tak by se za předpokladu chybějící vazby mezi směrovačem R2H a R4C, síť 7::/64 v tabulce vůbec nenacházela, protože cestou přes směrovač R3H a tudíž dvě IBGP vazby by se nedostala, znal by ji pouze směrovač R3H. Za stejného předpokladu chybějící vazby mezi R2H a R4C, bude naopak směrovač R4C postrádat informace o sítích 1::/64 a 5::/64.

Směrovací tabulka s informacemi z BGP protokolu na prvku od společnosti Cisco vypadá následovně:

```
R4C#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, B - BGP
B   1::/64   [200/0]     via 3::1
B   2::/64   [200/0]     via 3::1
C   3::/64   [0/0]       via ::, FastEthernet0/1
C   4::/64   [0/0]       via ::, FastEthernet0/0
```

```
B    5::/64    [200/0]     via 1::1
B    6::/64    [200/0]     via 4::1
C    7::/64    [0/0]       via ::, Loopback0
```

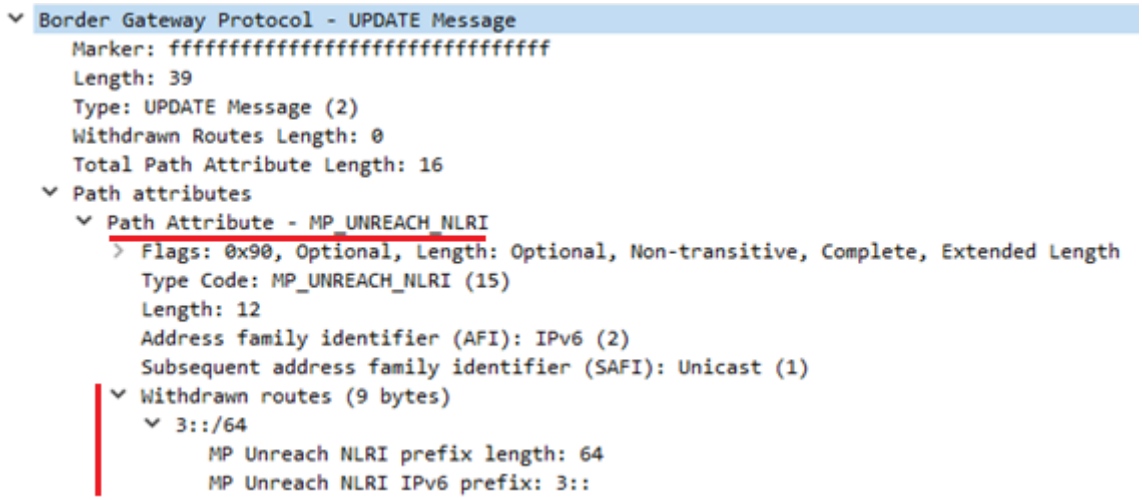
Na obrázku 3.14 je zobrazena zpráva OPEN, která je vytvořena každým směrovačem při vytváření vazby se sousedem. V této zprávě najdeme informace o verzi protokolu - 4, číslo AS, do kterého směrovač patří – 65010, dobu „Hold Time“, která udává, jak dlouho si směrovač bude spojení pamatovat v případě chybějících KEEPALIVE zpráv od souseda, po uplynutí této doby považuje spojení za nefunkční, a v neposlední řadě obsahuje také identifikační číslo směrovače, který zprávu vytvořil – 1.1.1.1, to odpovídá směrovači R1C. Zpráva obsahuje i dodatkové parametry jako jsou hodnoty AFI a SAFI (podrobněji vysvětleno v kapitole 1.5.3 Podpora IPv6).



Obrázek 3.14: OPEN zpráva protokolu BGP odchycená v programu Wireshark.

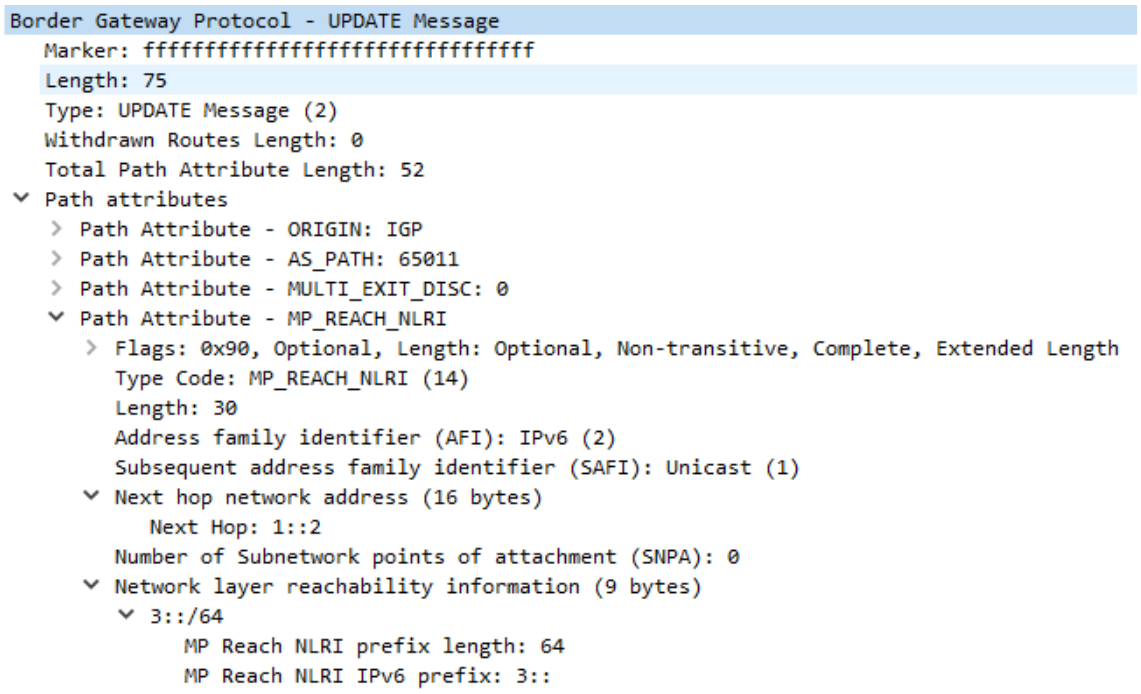
Obrázek 3.15 zobrazuje zachycenou UPDATE zprávu. Zprávy UPDATE jsou využívány k přenosu směrovacích informací o dostupných sítích ve formě prefixu sítě a jeho délky. Mimo tuto informaci se v těchto zprávách přenáší i několik atributů, které bývají přiřazeny k jednotlivým cestám. V neposlední řadě jsou zprávy UPDATE využívány k informaci o již neexistujících cestách, a to za pomocí atributu MP_UNREACH_NLRI a sekci „Withdrawn routes“. Právě tento případ je zachycen na obrázku 3.15. Ve zprávě jsou opět vypsány hodnoty AFI a SAFI, a v sekci „Withdrawn routes“ je obsažena síť s prefixem 3::/64. Aby došlo k této reakci a vytvoření zprávy UPDATE obsahující informace o neplatných cestách, byla při testování rozpojena linka mezi směrovačem R2H a R4C. Téměř okamžitě po zprávě obsahující informaci

o nedostupné síti 3::/64, byla odeslána další zpráva obsahující informaci o nedostupnosti sítě 7::/64.



Obrázek 3.15: Zpráva UPDATE protokolu BGP obsahující neplatné cesty.

Na obrázku 3.16 je zobrazena zpráva UPDATE obsahující hned několik atributů. Atribut ORIGIN označuje, že původ této směrovací informace pochází z IGP protokolu, resp. je tato cesta vzhledem k AS, ze kterého pochází, interní. Další atribut udává čísla AS, kterými zpráva prošla. Zde se jedná pouze o jedno číslo - 65011, neboť v tomto AS byla tato zpráva vygenerována. Atribut MULTI_EXIT_DISC se využívá k preferenci konkrétní cesty do AS v případě, že je cest více. V tomto konkrétním případě je mezi oběma AS pouze jedna cesta, a tak je tento atribut prázdný. Posledním atributem je opak toho z obrázku 3.15, a informuje nás o nově dostupné síti 3::/64.



Obrázek 3.16: Zpráva UPDATE obsahující několik atributů.

Konektivita spojení byla ověřována v průběhu testování programem PING z lokálních počítačů. Obrázek 3.17 znázorňuje zachycené pakety programem Wireshark z PC1(5::10) na PC2(6::10).

No.	Time	Source	Destination	Protocol	Length	Info
1805	717.485876	5::10	6::10	ICMPv6	118	Echo (ping) request id=0x0adb
1806	717.486174	6::10	5::10	ICMPv6	118	Echo (ping) reply id=0x0adb,

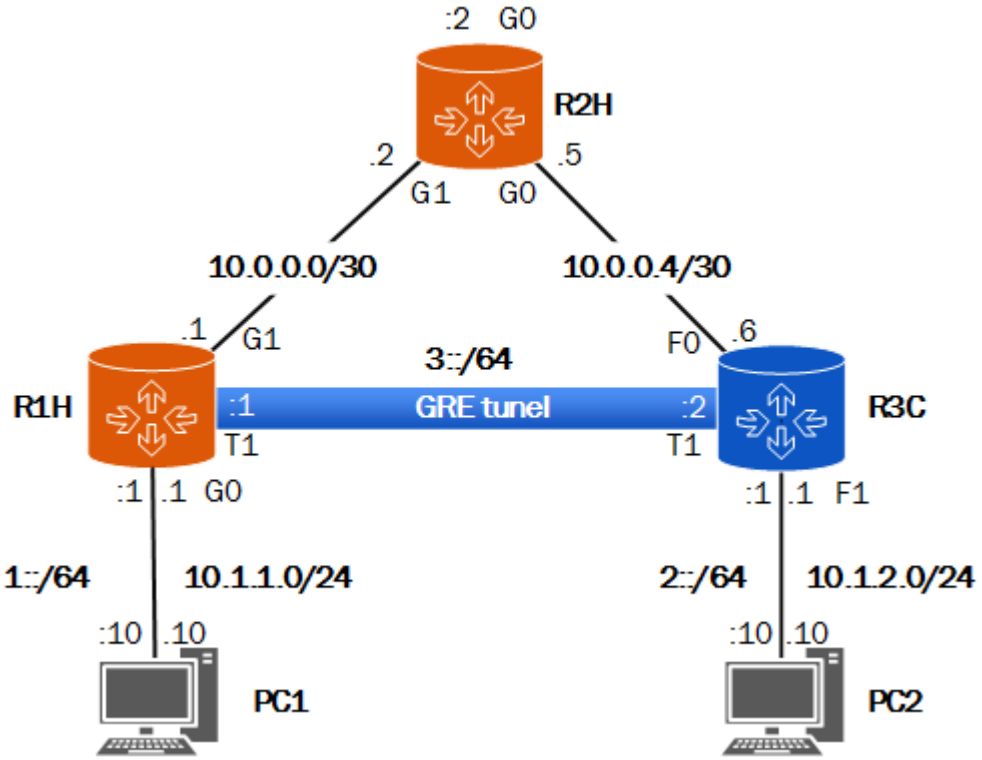
Obrázek 3.17: Pakety protokolu ICMPv6 zachycené programem Wireshark.

4 Praktické ověření koexistence zařízení pro IPv4 a IPv6

Stejně jako testování směrovacích protokolů i ověřování koexistence zařízení pro IPv4 a IPv6 probíhalo ve školní laboratoři na stejných zařízeních. Pro ověření kompatibility mezi zařízeními Huawei a prvky společnosti Cisco, byla testovaná topologie (viz. Obrázek 4.1) sestavena z prvků obou těchto výrobců. Jelikož je technologií pro koexistenci IPv6 a IPv4 protokolů spousta, což by vydalo na samostatnou práci, tak pro praktické ověření byl vybrán pouze jeden typ, který se nazývá IPv6 přes IPv4 manuální GRE tunel. Jaká byla použita topologie, a jaké konfigurace bylo na jednotlivých prvcích potřeba využít je sepsáno v následující kapitole 4.1 IPv6 přes IPv4 manuální GRE tunel.

4.1 IPv6 přes IPv4 manuální GRE tunel

Tunel GRE je založený na protokolu Generic Routing Encapsulation od společnosti Cisco. Tato technologie dokáže zapouzdřit širokou škálu protokolů síťové vrstvy do virtuálního spoje typu bod-bod neboli takzvaného tunelu, a to na bázi IPv4 protokolu. V praxi to znamená, že do přenášeného IPv4 paketu je, za jeho IPv4 hlavičku vložena hlavička protokolu GRE, za kterou pak následuje hlavička přenášeného protokolu, v tomto případě se bude jednat o IPv6 datagramy (viz. Obrázek 2.4).



Obrázek 4.1: Topologie pro otestování funkce IPv6 přes IPv4 manuální GRE tunel

4.1.1 Konfigurace

Abychom mohli tunelovat IPv6 pakety přes IPv4 síť, prvním krokem v konfiguraci je nastavit právě IPv4 síť. To znamená, že je na všech směrovačích a koncových zařízeních nutné nakonfigurovat IPv4 adresy. Jakmile jsou IPv4 adresy všude správně nakonfigurovány, a základní konektivita mezi jednotlivými prvky je funkční, můžeme přejít k dalšímu kroku konfigurace – směrování. Aby byly obě koncové sítě navzájem dostupné, je nutné zajistit alespoň statické směrování, či zvolit nějaký ze směrovacích protokolů. Já jsem si pro tento úkol zvolil protokol OSPF. Jelikož všechny úkony popsány v tomto odstavci jsou poměrně jednoduché, příkazy k jejich konfiguraci jsou shrnuty v následujícím výpisu. Následující postup konfigurace se vztahuje na směrovač R1H od společnosti Huawei.

```
[Huawei] sysname R1H
[R1H] interface GigabitEthernet0/0/0
[R1H-GigabitEthernet0/0/0] ip address 10.1.1.1 255.255.255.0
[R1H-GigabitEthernet0/0/0] quit
[R1H-GigabitEthernet0/0/1] ip address 10.0.0.1 255.255.255.252
[R1H-GigabitEthernet0/0/1] quit
[R1H] ospf 1
[R1H-ospfv-1] area 0
[R1H-ospfv-1-area-0.0.0.0] network 10.0.0.0 0.0.0.3
[R1H-ospfv-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

Koncová síť 10.1.1.0/24 na směrovači R1H, a síť 10.1.2.0/24 směrovače R3C nejsou pro správnou funkci tunelu GRE nutné, v této konfiguraci však byly zahrnuty pro demonstraci funkce obou protokolů (IPv4/IPv6) na jedné topologii zároveň. Analogicky nastavíme i zbylé dva směrovače, po té by měla být základní síť na bázi protokolu IPv4 funkční, a PC1 a PC2 by měly být navzájem dostupné pomocí programu PING.

Nyní přejdeme ke konfiguraci části sítě, která poběží na protokolu IPv6. Jedná se o koncové sítě 1::/64 a 2::/64. Abychom mohli využívat IPv6 protokol, je potřeba použít příkazy, které tento protokol na směrovači povolí.

```
[R1H] ipv6
[R1H] interface GigabitEthernet0/0/0
[R1H-GigabitEthernet0/0/0] ipv6 enable
[R1H-GigabitEthernet0/0/0] ipv6 address 1::1 64
[R1H-GigabitEthernet0/0/0] quit
```

IPv6 adresy je potřeba nastavit i na koncových stanicích PC1 (1::10/64) a PC2 (2::10/64). V této fázi jsou nakonfigurovány dvě IPv6 sítě, které jsou od sebe oddělené. Abychom tyto sítě

propojili, musíme nakonfigurovat tunel, který IPv6 pakety zapouzdří a přenese přes IPv4 část sítě. Tunel vytvoříme následujícím příkazem:

```
[R1H] interface tunnel 0/0/1
```

Nyní musíme nastavit parametry tunelu, a to povolit IPv6 protokol, nastavit IPv6 adresu, nastavit mód tunelu, neboli používaný protokol – GRE.

```
[R1H-Tunnel0/0/1] tunnel-protocol gre
[R1H-Tunnel0/0/1] ipv6 enable
[R1H-Tunnel0/0/1] ipv6 address 3::1 64
```

Na opačném konci tunelu je nastavena IPv6 adres 3::2/64. Poslední, ale za to velice důležité příkazy udávají zdroj a cíl tunelu, neboli IPv4 adresy rozhraní, kde bude tunel začínat, a kde končit. Počátkem tunelu, kde se přenášené pakety zapouzdří, je rozhraní G1 směrovače R1H s IPv4 adresou 10.0.0.1. Konec tunelu je na umístěn na rozhraní F0 s IPv4 adresou 10.0.0.6 na směrovači R3C. Směrovač R2H, který je umístěn na trase tunelu mezi jeho počátkem a koncem, pouze směruje pakety jako při standardním IPv4 provozu. Zdroj a cíl tunelu nastavíme následujícími příkazy:

```
[R1H-Tunnel0/0/1] source 10.0.0.1
[R1H-Tunnel0/0/1] destination 10.0.0.6
[R1H-Tunnel0/0/1] quit
```

Na směrovači R3C, jsou IPv4 adresy těchto dvou příkazů – zdroj a cíl, pouze přehozeny. Po vytvoření tunelu musíme nastavit směrování, aby směrovače R1H a R3C vzájemně znaly cestu do svých koncových IPv6 sítí. K tomu nám stačí nastavit statické IPv6 cesty. Použijeme následující příkazy:

```
[R1H]ipv6 route-static 2:: 64 Tunnel0/0/1
R3C(config)# ipv6 route 1::/64 Tunnel1
```

Po nastavení statických cest je konfigurace kompletní a obě koncové IPv6 sítě jsou vzájemně dostupné.

4.1.2 Ověření konfigurace

V této kapitole naleznete zejména příkazy a jejich výpisy, pomocí kterých je možné zkontrolovat správnou funkčnost protokolu a informace o topologii.

Abychom věděli, zda je tunel správně nakonfigurován, velmi užitečný je příkaz pro zobrazení souhrnných informací o konkrétním tunelovém rozhraní:

```
[R1H]display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.0.1 (GigabitEthernet0/0/1), destination
10.0.0.6
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
```

Výpis nám udává aktuální stav tunelu, informace o zapouzdřování, MTU, IPv4 adresu zdroje i cíle, rozhraní zdroje a také tunelovací protokol, který je v konfiguraci použit.

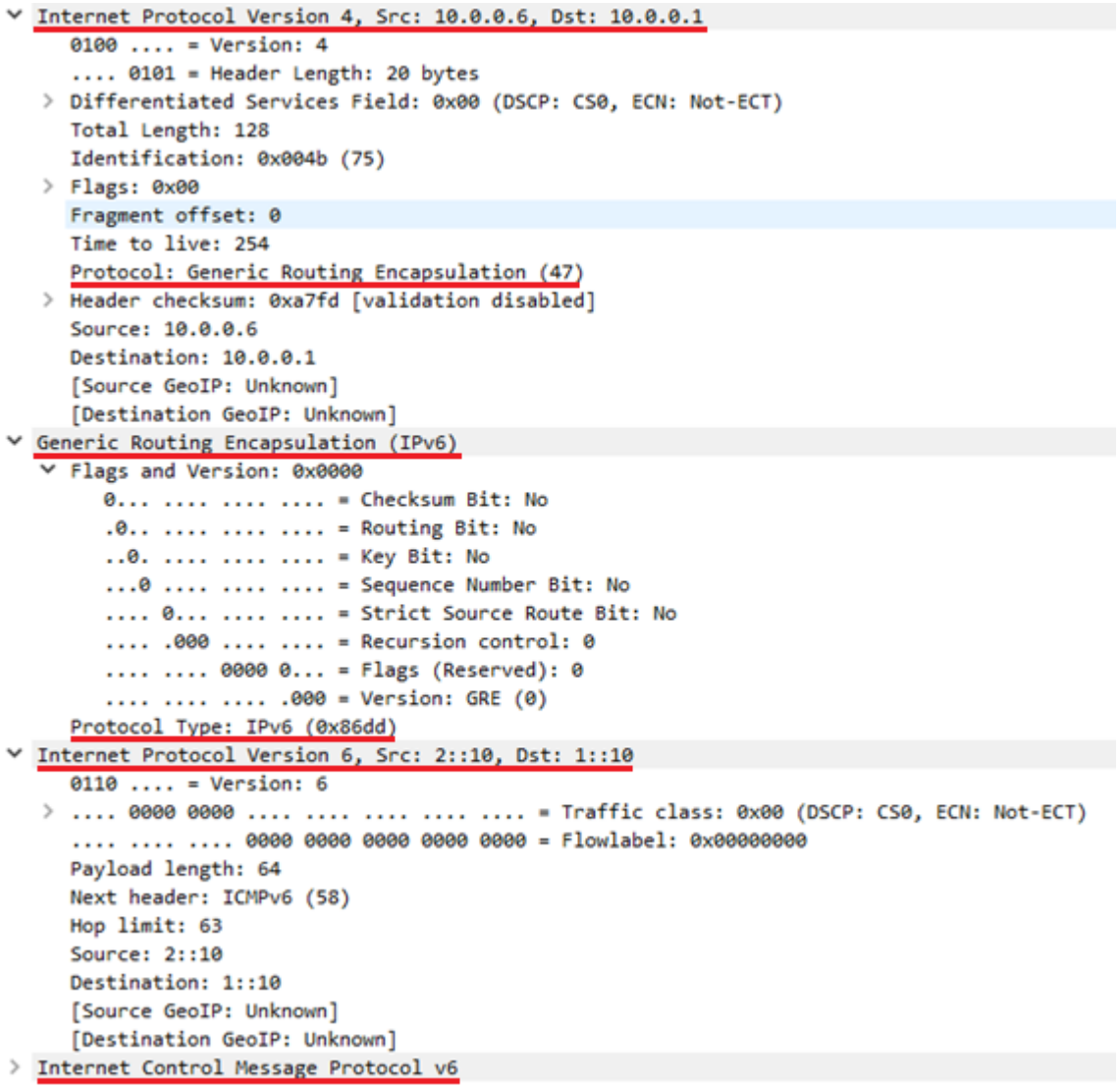
Dále výpis směrovací tabulky jasně ukazuje, že síť 2::/64 je dostupná přes rozhraní Tunnel0/0/1.

```
 Destination  : 2::                        PrefixLength : 64
 NextHop      : 3::1                       Preference   : 60
 Cost         : 0                          Protocol     : Static
 RelayNextHop : ::                         TunnelID     : 0x0
 Interface    : Tunnel0/0/1                Flags        : D
```

Na Obrázku 4.2 je znázorněn zapouzdřený IPv6 paket odchycený programem Wireshark. Dle pořadí vidíme, že odchycený paket obsahuje celkem čtyři hlavičky. První je hlavička IPv4 protokolu, která nese informaci v podobě IPv4 adresy o zdroji (10.0.0.6) a cíli (10.0.0.1). Jako další informaci zde nalezneme, že přenášený protokol je GRE, jehož identifikační číslo je 47, např. ICMP má číslo 1, TCP = 6, UDP = 17.

Co se týče samotného GRE protokolu, ten moc informací ke zhlédnutí nenabízí kromě pole, které je nazváno „Protocol Type:“. Toto pole má celkovou délku 16 bitů, a udává jaký protokol je zapouzdřen pomocí protokolu GRE. Dle obrázku se jedná o protokol IPv6, jehož hodnota EtherType je 0x86dd (viz. Kapitola 2.1 Technologie Dual Stack). Další v řadě je hlavička

protokolu IPv6, který obsahuje zdrojovou a cílovou IPv6 adresu a informace o poslední hlavičce, kterou je ICMPv6 protokol, který používá program PING6. Tímto způsobem je tedy řešený přenos IPv6 paketů přes IPv4 manuální GRE tunel.



Obrázek 4.2: IPv6 paket zapouzdřený protokolem GRE.

5 Rozdíly a kompatibilita směrovačů Huawei a Cisco

Podklady pro praktickou část této diplomové práce byly získány při testování, zkoušení a ověřování různých funkcí na fyzických zařízeních Huawei a Cisco, které jsou dostupné ve školní laboratoři POREB215. Mezi prvky společnosti Huawei byly k dispozici tyto tři směrovače:

- AR1220V
- AR2220
- AR3260

Každý z těchto směrovačů patří do jiné výkonnostní řady, přičemž nejvýkonnější, i rozměrově největší z testovaných směrovačů je model AR3260. Nejslabší model, který byl v laboratoři k dispozici, nese označení AR1220V. Tento směrovač je rozměrově menší než klasické směrovače, které se montují do standardního racku. Většina z vybavení na předním panelu je pevně daná, a nelze ji nijak upravit. Nabízí pouze dva modulární sloty, pomocí kterých můžeme směrovač doplnit kompatibilními rozšiřujícím kartami. Využití tohoto směrovače je především v malých sítích, kde není generován příliš velký provoz. Dalším modelem je AR2220. Je to směrovač klasických rozměrů, který zabere v racku pozici velikosti 1U. Jeho výkon je o něco lepší než u prvního modelu, nicméně cenově se tyto dva směrovače příliš neliší. Za to třetí model je 4x až 6x dražší v závislosti na jeho konfiguraci. V racku zasahuje 3U pozice, nabízí mnohem výkonnější hardware a především spoustu modulárních slotů. Tento směrovač najde využití ve velkých sítích, jaké najdeme uvnitř velkých korporací, školních kampusů či u poskytovatelů internetového připojení. Všechny tři směrovače Huawei jsou vybaveny porty typu Gigabit Ethernet, které, jak už název napovídá, disponují přenosovou rychlostí až 1 Gbit/s. Poměrně užitečným doplňujícím prvkem byl fyzický kolébkový přepínač pro vypnutí/zapnutí napájecího zdroje směrovače.

Od společnosti Cisco byly v jednotlivých topologiích využity zařízení z řady 2800. Tyto směrovače nabízí pouze porty typu Fast Ethernet, jejichž rychlost je 100 Mbit/s, tedy 10x nižší než u testovaných prvků Huawei. Co se týče stránky programového vybavení prvků, u systému VRP od společnosti Huawei je „cítit“ poměrně silná inspirace systémem IOS společnosti Cisco, nicméně toto nepovažuji za mínus, nýbrž výhodu, protože je konfigurace jednotlivých funkcí poměrně podobná. Systém VRP má oproti systému IOS pouze dvě úrovně pro zadávání příkazů, což v dlouhodobém užívání podstatně šetří čas uživatele, nicméně IOS je naproti tomu striktněji rozdělený na čistě konfigurační úroveň a úroveň, na které můžeme získat všemožné výpisy informací. Konkrétní příkazy pro konfiguraci určitých funkcí se ve většině případech mírně odlišují, to však někdy práci při konfiguraci ulehčí, někdy naopak přidá.

Jelikož se tato práce věnuje směrovačům a směrování obecně, je vhodné uvést rozdíly v preferenci cest jednotlivých směrovacích protokolů před ostatními. Ve výpisech prvků Huawei najdeme hodnotu „preference“, Cisco tomu naopak říká „administrative distance“. V obou případech se jedná o jednu a tu samou hodnotu. Tato hodnota je číslo v rozmezí 0-255, kdy menší znamená vyšší prioritu. Určuje, jak se směrovač rozhodne, bude-li mít ve své směrovací tabulce dvě cesty do stejné sítě, avšak každá bude pocházet z jiného směrovacího protokolu.

Zjednodušeně řečeno, jedná se o tabulku udávající prioritu jednotlivých cest. Tyto hodnoty se liší dle výrobce, který určuje, podle jaké priority se bude směrovač řídit. Přehled základních a nejpoužívanějších typů cest včetně jejich priority je shrnut v tabulce 5.1. Z uvedené tabulky vyplývá, že prvky Huawei si po přímo připojené síti nejvíce váží cest získaných z protokolu OSPF, který je následován protokolem IS-IS, a až na čtvrtém místě je statická cesta. Prvky společnosti Cisco si statické cesty označují prioritou 1, hned po přímo připojených sítích. Pak následují cesty pocházející z externího BGP protokolu a teprve potom z dynamických protokolů. Z těchto faktů vyplývá, že Cisco preferuje manuálně nakonfigurované statické cesty před těmi z dynamických protokolů. Společnost Huawei naopak preferuje dynamické protokoly OSPF a IS-IS před manuálně nakonfigurovanou statickou cestou a EBGP cestou.

Tabulka 5.1: Preference cest výrobců Huawei a Cisco. [18][19][20]

Typ/původ cesty	Huawei	Cisco
Přímo připojená síť	0	0
OSPF	10	110
IS-IS	15	115
Statická cesta	60	1
RIP	100	120
IBGP	255	200
EBGP	255	20

Při praktickém testování a ověřování jednotlivých směrovacích protokolů a dalších funkcí nebyly zjištěny žádné známky nekompatibility mezi zařízeními Huawei a Cisco. Tento fakt bych odůvodnil tím, že testované směrovací protokoly a funkce jsou mezinárodně definované standardy, a tudíž by jakákoliv vada porušovala nejen tyto standardy, nýbrž by i poškozovala samotného výrobce, jehož výrobky by byly takzvaně nefunkční či funkční pouze v omezené míře.

Závěr

Cílem této diplomové práce bylo popsat směrovací protokoly využívané v sítích založených na protokolu IPv6, návrh a realizace topologií k jejich otestování v laboratorním prostředí s využitím směrovačů Huawei. V druhé části pak popsat a prakticky ověřit řešení umožňující koexistenci protokolů IPv4 a IPv6. Závěrem pak porovnat a ověřit kompatibilitu směrovačů Huawei a Cisco.

V laboratoři byly k dispozici pro testování tři směrovače společnosti Huawei. Konkrétně modely – AR1220V, AR2220 a AR3260. Každý z těchto modelů patří do jiné produktové řady, což znamená, že se každý liší jak svými parametry a nabízeným výkonem, tak i oblastí využití.

Do testování v laboratoři byly zapojeny i směrovače Cisco řady 2800. Jedná se o zařízení staršího data výroby než prvky Huawei, které byly k dispozici. Z toho důvodu nabízejí pomalejší porty, nicméně se pořád jedná o velmi kvalitní zařízení.

Na různých topologiích byly otestovány celkem 4 různé směrovací protokoly pro IPv6. Prvním byl protokol RIPng, který je vhodný pro využití v menších sítích, jelikož je náchylný k tvorbě smyček v sítí a v rozlehlých sítích je velmi špatně odhaluje. Pro svou jednoduchost je však velmi oblíben v malých nenáročných sítích. Následován byl protokolem OSPFv3. Tento protokol nabízí hierarchii v podobě oblastí, do kterých lze fyzickou síť rozdělit. Topologie pro otestování tohoto protokolu obsahovala redistribuci směrovacích informací ze směrovacího protokolu RIPng, to zejména proto, aby bylo ověřeno chování všech možných typů oblastí protokolu OSPFv3 včetně zasílání různých druhů LSA zpráv. Další testovaný směrovací protokol byl IS-IS. Tento směrovací protokol je pro svou univerzálnost oblíben především u náročnějších a složitějších sítí. Je poměrně podobný protokolu OSPFv3, a také nabízí hierarchii v podobě oblastí, nicméně pouze dvou typů – L1 a L2. Cílem testované topologie bylo ověřit chování jednotlivých typů směrovačů v topologii – L1, L2 a L1/L2. Například směrovače L1/L2, které leží na hranici obou oblastí, si udržují dvě směrovací tabulky, jednu pro oblast L1, druhou pro oblast L2. Z toho důvodu by měly tyto směrovače disponovat větším výpočetním výkonem než zbylé typy, jelikož provádí SPF výpočet 2x, namísto jednou. Posledním testovaným směrovacím protokolem byl BGP4+. BGP4+ se od předešlých směrovacích protokolů liší tím, že je určen především pro směrování mezi autonomními systémy na páteřních sítích. Směrovací tabulka takového prvku může obsahovat až tisíce různých cest. Cílem testované topologie bylo ověřit funkci jak externích, tak interních BGP vazeb a ochranu proti vzniku smyček uvnitř autonomního systému.

Jak již bylo zmíněno výše, testované topologie byly postaveny ze směrovačů Huawei a Cisco. Směrovače obou těchto společností byly záměrně zapojeny tak, aby musely společně komunikovat a spoléhat se jeden na druhého v předávaných informacích. Během testování však nebyly objeveny žádné známky nekompatibility, či špatné komunikace, a to zejména z toho důvodu, že všechny testované směrovací protokoly jsou mezinárodními standardy, a tudíž jsou využívány celou řadou výrobců, kteří by zároveň měli zaručit jejich správnou funkci bez ohledu

na to, od jakého výrobce pochází směrovač, se kterým je v síti potřeba komunikovat a vyměňovat si informace.

Nicméně jeden podstatný rozdíl mezi směrovači Huawei a Cisco zde je. Jedná se o prioritu cest pocházejících z různých směrovacích protokolů. V situaci, kdy má směrovač do jedné sítě dvě cesty, kde každá z nich byly získána přes jiný směrovací protokol, se směrovač rozhoduje podle předem nastavené priority, což je ve většině případů číslo od 0 do 255. Tuto prioritu, kterou naopak Cisco nazývá administrativní vzdálenost, udává výrobce, a tak se tyto hodnoty mezi směrovači různých výrobců mohou lišit. Tyto hodnoty lze během konfigurace manuálně upravit. V základním nastavení však směrovače Huawei upřednostňují spíše dynamické protokoly (OSPF, IS-IS) před statickou cestou. Naopak směrovače Cisco upřednostňují před dynamickými protokoly manuálně nakonfigurovanou statickou cestu, či EBGP protokol. Vzhledem k tomuto faktu, je potřeba dávat pozor při práci se sítěmi, které jsou postaveny ze směrovačů různých výrobců a dle potřeby dané hodnoty priorit poupravit tak, aby byla směrovací politika celé sítě jednotná.

Řešení koexistence zařízení pro IPv4 a IPv6 má mnoho způsobů. Základem je však podpora protokolu IPv6 u jednotlivých zařízení využívaných v síti, včetně směrovačů. Jedním z řešení, které bylo otestováno v laboratoři, byla technologie IPv6 přes IPv4 manuální GRE tunel. Tato technologie je založena na protokolu Generic Routing Encapsulation, který je původně vyvinutý společností Cisco a dokáže zapouzdřit a přes virtuální tunel přenést různé protokoly 3. vrstvy modelu ISO/OSI, včetně protokolu IPv6. Cílem bylo ověřit podporu tohoto protokolu u směrovačů Huawei, které si s tímto protokolem poradily bez jakýchkoli problémů.

Programové vybavení prvků Huawei a Cisco se pro své uživatele jeví velice podobně, nicméně určité odlišnosti zde najdeme, ať už se jedná o počet základních konfiguračních úrovní pro zadávání příkazů, či o konfiguraci konkrétních funkcí směrovačů. Vše pak záleží na konkrétním uživateli, co mu více vyhovuje. Z mého osobního pohledu si systém VRP od Huawei nevede úplně špatně, co se týče uživatelské přívětivosti. Mnoho funkcí a konfiguračních způsobů se mi jeví lépe řešených než u systému IOS společnosti Cisco, se kterým jsem měl možnost pracovat již několik let. Přes všechny klady systému VRP, mi systém IOS přijde mnohem profesionálnější, ať už z pohledu množství a přehlednosti informací, které můžeme při konfiguraci prvků vypsat, či v možnostech konfigurace jednotlivých funkcí.

Použitá literatura

[1] IPv6. [online]. [cit. 2015-01-30]. Dostupné z: http://en.wikipedia.org/wiki/IPv6

[2] IPv6. [online]. [cit. 2015-01-30]. Dostupné z: http://www.fi.muni.cz/~kas/p090/referaty/2005-podzim/ct/ipv6.html

[3] IPv6 multicast. [online]. [cit. 2015-01-30]. Dostupné z: http://ipv6friday.org/blog/2011/12/ipv6-multicast/

[4] RIPng Overview. [online]. [cit. 2015-01-30]. Dostupné z: http://www.juniper.net/techpubs/en_US/junos14.1/topics/concept/routing-protocol-rip-ng-security-overview.html

[5] RIPng. [online]. [cit. 2015-01-30]. Dostupné z: https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ripng

[6] OSPF for IPv6. [online]. [cit. 2015-02-03]. Dostupné z: http://tools.ietf.org/html/rfc5340#section-2

[7] Implementing OSPFv6. [online]. [cit. 2015-02-03]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-ospf.html#GUID-DCB20ADF-1F8E-434B-AE97-54802879F34F

[8] OSPFv3 LSA Types. [online]. [cit. 2015-02-03]. Dostupné z: https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ospf

[9] IS-IS Network Protocol Basics. [online]. [cit. 2015-02-03]. Dostupné z: http://www.dummies.com/how-to/content/isis-network-protocol-basics.html

[10] Intermediate System-to-Intermediate System Protocol. [online]. [cit. 2015-02-21]. Dostupné z: http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml#wp38591

[11] Routing Protocol - IS-IS. [online]. [cit. 2015-02-21]. Dostupné z: http://www.interlab.ait.ac.th/tein2/Presentations/Basic%20Routing/IS-IS%20-%20Routing%20Protocol.pdf

[12] IS-IS for IPv6 Technology White Paper. [online]. [cit. 2015-02-21]. Dostupné z: https://www.h3c.com/portal/download.do?id=625934

[13] IPv6 Advanced Protocols Implementation part 1[online]. [cit. 2016-01-23]. Dostupné z: http://what-when-how.com/ipv6-advanced-protocols-implementation/introduction-to-bgp4-ipv6-unicast-routing-protocols-part-1/

[14] IPv6 Advanced Protocols Implementation part 2 [online]. [cit. 2016-01-23]. Dostupné z: http://what-when-how.com/ipv6-advanced-protocols-implementation/introduction-to-bgp4-ipv6-unicast-routing-protocols-part-2/

[15] BGP [online]. [cit. 2016-01-23]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

[16] Techniky a řešení paralelního fungování a přechodů mezi IPv4 a IPv6 [online]. [cit. 2016-03-31]. Dostupné z: http://www.netguru.cz/odborne-clanky/techniky-a-eeni-paralerniho-fungovani-a-pechodu-z-v4-a-v6.html

[17] Support Huawei [online]. [cit. 2016-03-31]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000019444&partNo=10022

[18] Route preference [online]. [cit. 2016-04-07]. Dostupné z: http://carnivalpeanutbutter.blogspot.cz/2013/08/as-promised-below-are-route-preference.html

[19] Huawei route preference [online]. [cit. 2016-04-07]. Dostupné z: https://labnario.files.wordpress.com/2012/10/huawei-route-preferences.pdf

[20] Administrative distance [online]. [cit. 2016-04-07]. Dostupné z: https://en.wikipedia.org/wiki/Administrative_distance

[21] TEARE, Diane, et al. *CCNP Routing and Switching Foundation Learning Library: Foundation Learning for CCNP ROUTE, SWITCH, and TSHOOT (642-902, 642-813, 642-832).* 1st ed. Indianapolis: Cisco Press, 2010. ISBN-13: 978-1-58705-885-1.

Seznam obrázků

Seznam příloh

Příloha A: *Konfigurace a výpisy ke kapitole 3.1 Směrování pomocí RIPng*

Tato příloha obsahuje konfiguraci a důležité výpisy z vybraných zařízení. Především se jedná o alespoň jedno zařízení od každého výrobce, popř. ostatních zařízení, které v konfiguraci hrály nezbytnou roli. Některé konfigurační výpisy byly zkrácené z důvodu příliš zdlouhavého výpisu.

Směrovač R3H – Huawei:

- **Výpis konfigurace RIPng:**

```
[R3H]display current-configuration
[V200R003C00SPC200]
#
 sysname R3H
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 2::2/64
 ripng 1 enable
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 4::2/64
 ripng 1 enable
#
interface GigabitEthernet0/0/2
 ipv6 enable
 ipv6 address 6::1/64
 ripng 1 enable
#
ripng 1
#
Return
```

- **Výpis směrovací tabulky:**

```
[R3H]display ipv6 routing-table
Routing Table : Public
        Destinations : 11       Routes : 12

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : FE80::217:5AFF:FE4B:5358     Preference   : 100
 Cost         : 1                            Protocol     : RIPng
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::                          PrefixLength : 64
 NextHop      : 2::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::2                         PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 3::                          PrefixLength : 64
 NextHop      : FE80::217:5AFF:FE4B:5821     Preference   : 100
```

```
Cost         : 1                          Protocol     : RIPng
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 4::                        PrefixLength : 64
NextHop      : 4::2                       Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 4::2                       PrefixLength : 128
NextHop      : ::1                        Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 5::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5358   Preference   : 100
Cost         : 2                          Protocol     : RIPng
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 5::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5821   Preference   : 100
Cost         : 2                          Protocol     : RIPng
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 6::                        PrefixLength : 64
NextHop      : 6::1                       Preference   : 0
Cost         : 0                          Protocol     : Direct
```

```
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2         Flags        : D

Destination  : 6::1                         PrefixLength : 128
NextHop      : ::1                          Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2         Flags        : D

Destination  : FE80::                       PrefixLength : 10
NextHop      : ::                           Preference   : 0
Cost         : 0                            Protocol     : Direct
RelayNextHop : ::                           TunnelID     : 0x0
Interface    : NULL0                        Flags        : D
```

Směrovač R2C – Cisco:

- **Výpis konfigurace RIPng:**

```
R2C#sh running-config
Building configuration...

Current configuration : 1309 bytes
version 12.4
!
hostname R2C
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 1::2/64
 ipv6 enable
 ipv6 rip 1 enable
!
ipv6 router rip 1
End
```

- **Výpis směrovací tabulky:**

```
R2C#sh ipv6 route
IPv6 Routing Table - Default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D -
EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   1::/64 [0/0]
     via FastEthernet0/1, directly connected
L   1::2/128 [0/0]
     via FastEthernet0/1, receive
C   2::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2::1/128 [0/0]
     via FastEthernet0/0, receive
R   3::/64 [120/2]
     via FE80::A19:A6FF:FE9B:6D4F, FastEthernet0/1
R   4::/64 [120/2]
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
R   5::/64 [120/2]
     via FE80::A19:A6FF:FE9B:6D4F, FastEthernet0/1
R   6::/64 [120/2]
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Příloha B: *Konfigurace a výpisy ke kapitole 3.2 Směrování pomocí OSPFv3*

Tato příloha obsahuje konfiguraci a důležité výpisy z vybraných zařízení. Především se jedná o alespoň jedno zařízení od každého výrobce, popř. ostatních zařízení, které v konfiguraci hrály nezbytnou roli. Některé konfigurační výpisy byly zkrácené z důvodu příliš zdlouhavého výpisu.

Směrovač R3H – Huawei:

- **Výpis konfigurace OSPFv3:**

```
[R3H]display current-configuration
[V200R003C00SPC200]
#
 sysname R3H
#
ipv6
#
ospfv3 1
 router-id 3.3.3.3
 default cost 25
 import-route ripng 1 type 2
 area 0.0.0.2
  nssa
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 2::2/64
 ospfv3 1 area 0.0.0.2
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 4::2/64
 ripng 1 enable
#
```

```
ripng 1
 default-cost 5
 import-route ospfv3 1
```

- **Výpis směrovací tabulky:**

```
[R3H]display ipv6 routing-table
Routing Table : Public
        Destinations : 10       Routes : 10

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : FE80::217:5AFF:FE4B:5358     Preference   : 10
 Cost         : 2                            Protocol     : OSPFv3
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::                          PrefixLength : 64
 NextHop      : 2::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::2                         PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
```

```
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 3::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5358   Preference   : 10
Cost         : 3                          Protocol     : OSPFv3
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 4::                        PrefixLength : 64
NextHop      : 4::2                       Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 4::2                       PrefixLength : 128
NextHop      : ::1                        Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                        TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1      Flags        : D

Destination  : 5::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5358  Preference   : 10
Cost         : 4                          Protocol     : OSPFv3
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0      Flags        : D

Destination  : 6::                        PrefixLength : 64
NextHop      : FE80::21E:F7FF:FEAC:4A63  Preference   : 100
Cost         : 1                          Protocol     : RIPng
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1      Flags        : D
```

```
 Destination  : FE80::                    PrefixLength : 10
 NextHop      : ::                        Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                        TunnelID     : 0x0
 Interface    : NULL0                     Flags        : D
```

- **Výpis informací o směrovacím protokolu OSPFv3:**

```
[R3H]display ospfv3 1
 Routing Process "OSPFv3 (1)" with ID 3.3.3.3
 Route Tag: 0
 Multi-VPN-Instance is not enabled
 SPF Intelligent Timer[millisecs] Max: 10000, Start: 500, Hold:
2000
 LSA Intelligent Timer[millisecs] Max: 5000, Start: 500, Hold:
1000
 LSA Arrival interval 1000 millisecs
 Default ASE parameters: Metric: 25 Tag: 1 Type: 2
 Number of AS-External LSA 0. AS-External LSA's Checksum Sum
0x0000
 Number of AS-Scoped Unknown LSA 0. AS-Scoped Unknown LSA's
Checksum Sum 0x0000
 Number of FULL neighbors 1
 Number of Exchange and Loading neighbors 0
 Number of LSA originated 5
 Number of LSA received 12
 SPF Count          : 0
 Non Refresh LSA    : 0
 Non Full Nbr Count : 0
 Number of areas in this router is 1
```

Směrovač R2C – Cisco:

- **Výpis konfigurace OSPFv3:**

```
R2C#sh running-config
Current configuration : 1469 bytes
version 12.4
!
hostname R2C
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 enable
 ipv6 ospf 1 area 2
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 1::2/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 area 2 nssa
```

```
line con 0
 logging synchronous
```

- **Výpis směrovací tabulky:**

```
R2C#sh ipv6 route
IPv6 Routing Table - Default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route, B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1, I2 - ISIS L2,
IA - ISIS interarea, IS - ISIS summary, D – EIGRP, EX - EIGRP
external, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2
- OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   1::/64 [0/0]
     via FastEthernet0/1, directly connected
L   1::2/128 [0/0]
     via FastEthernet0/1, receive
C   2::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2::1/128 [0/0]
     via FastEthernet0/0, receive
OI  3::/64 [110/2]
     via FE80::A19:A6FF:FE9B:6D4F, FastEthernet0/1
ON2 4::/64 [110/25], tag 1
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
OI  5::/64 [110/3]
     via FE80::A19:A6FF:FE9B:6D4F, FastEthernet0/1
ON2 6::/64 [110/25], tag 1
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
```

- **Výpis informací o směrovacím protokolu OSPFv3:**

```
R2C#sh ipv6 ospf 1
 Routing Process "ospfv3 1" with ID 2.2.2.2
 It is an area border and autonomous system boundary router
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 2. Checksum Sum 0x00FC3F
 Number of areas in this router is 2. 1 normal 0 stub 1 nssa
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        SPF algorithm executed 13 times
        Number of LSA 9. Checksum Sum 0x042801
        Number of DCbitless LSA 2
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 2
        Number of interfaces in this area is 1
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        SPF algorithm executed 18 times
        Number of LSA 11. Checksum Sum 0x0341E4
        Number of DCbitless LSA 2
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Směrovač R4C – Cisco:

- **Výpis směrovací tabulky:**

```
R4C#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B – BGP, U
- Per-user Static route, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS
interarea, IS - ISIS summary, O - OSPF intra, OI - OSPF inter,
OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 -
OSPF NSSA ext 2
OI  ::/0 [110/2]
     via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
OI  1::/64 [110/2]
     via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
OI  2::/64 [110/3]
     via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
C   3::/64 [0/0]
     via ::, FastEthernet0/0
L   3::2/128 [0/0]
     via ::, FastEthernet0/0
C   5::/64 [0/0]
     via ::, FastEthernet0/1
L   5::1/128 [0/0]
     via ::, FastEthernet0/1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Příloha C: *Konfigurace a výpisy ke kapitole 3.3 Směrování pomocí IS-IS*

Tato příloha obsahuje konfiguraci a důležité výpisy z vybraných zařízení. Především se jedná o alespoň jedno zařízení od každého výrobce, popř. ostatních zařízení, které v konfiguraci hrály nezbytnou roli. Některé konfigurační výpisy byly zkrácené z důvodu příliš zdlouhavého výpisu.

Směrovač R1C – Cisco:

- **Výpis konfigurace IS-IS:**

```
R1C#show running-config
Version 12.4
!
hostname R1C
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 ipv6 address 2::1/64
 ipv6 enable
 ipv6 router isis 1
!
interface FastEthernet0/1
 ipv6 address 1::1/64
 ipv6 enable
 ipv6 router isis 1
!
router isis 1
 net 49.0010.1111.1111.1111.00
 is-type level-1
!
line con 0
 logging synchronous
```

- **Výpis směrovací tabulky:**

```
R1C#show ipv6 route

IPv6 Routing Table - Default - 7 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route, B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1, I2 - ISIS L2,
IA - ISIS interarea, IS - ISIS summary, D – EIGRP, EX - EIGRP
external, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2
- OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

I1 ::/0 [115/10] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0

C  1::/64 [0/0] via FastEthernet0/1, directly connected

L  1::1/128 [0/0] via FastEthernet0/1, receive

C  2::/64 [0/0] via FastEthernet0/0, directly connected

L  2::1/128 [0/0] via FastEthernet0/0, receive

I1 3::/64 [115/20] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0

L  FF00::/8 [0/0] via Null0, receive
```

Směrovač R2H – Huawei:

- **Výpis konfigurace IS-IS:**

```
[R2H]display current-configuration
[V200R005C20SPC200]
#
 sysname R2H
#
ipv6
#
isis 1
 network-entity 49.0010.2222.2222.2222.00
 #
 ipv6 enable topology standard
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 2::2/64
 isis ipv6 enable 1
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 3::1/64
 isis ipv6 enable 1
 isis authentication-mode simple plain Test
#
Return
```

- **Výpis směrovací tabulky:**

```
[R2H]display ipv6 routing-table
Routing Table : Public
        Destinations : 11       Routes : 11

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : FE80::217:5AFF:FE4B:5358     Preference   : 15
 Cost         : 20                           Protocol     : ISIS-L1
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::                          PrefixLength : 64
 NextHop      : 2::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 2::2                         PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 3::                          PrefixLength : 64
 NextHop      : 3::1                         Preference   : 0
```

```
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 3::1                       PrefixLength : 128
NextHop      : ::1                        Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 4::                        PrefixLength : 64
NextHop      : FE80::A19:A6FF:FE9A:8277   Preference   : 15
Cost         : 20                         Protocol     : ISIS-L2
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 5::                        PrefixLength : 64
NextHop      : FE80::A19:A6FF:FE9A:8277   Preference   : 15
Cost         : 30                         Protocol     : ISIS-L2
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 6::                        PrefixLength : 64
NextHop      : FE80::A19:A6FF:FE9A:8277   Preference   : 15
Cost         : 30                         Protocol     : ISIS-L2
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 7::                        PrefixLength : 64
NextHop      : FE80::A19:A6FF:FE9A:8277   Preference   : 15
Cost         : 40                         Protocol     : ISIS-L2
```

```
 RelayNextHop : ::                          TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1        Flags        : D

 Destination  : FE80::                      PrefixLength : 10
 NextHop      : ::                          Preference   : 0
 Cost         : 0                           Protocol     : Direct
 RelayNextHop : ::                          TunnelID     : 0x0
 Interface    : NULL0                       Flags        : D
```

- **Výpis databáze LS:**

```
[R2H]display isis lsdb

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                 Seq Num   Checksum Holdtime Length ATT/P/OL
-------------------------------------------------------------------------------
1111.1111.1111.00-00 0x0000000e 0xc6fa  654      103    0/0/0
2222.2222.2222.00-00* 0x00000014 0x534b 608      118    1/0/0
2222.2222.2222.01-00* 0x00000007 0xd7ef 608       55    0/0/0

Total LSP(s): 3
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self
LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload
```

Level-2 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL
2222.2222.2222.00-00*	0x0000001b	0xf04a	608	132	0/0/0
2222.2222.2222.02-00*	0x00000008	0x35c3	608	55	0/0/0
3333.3333.3333.00-00	0x00000014	0xde80	904	129	0/0/0
3333.3333.3333.02-00	0x00000008	0x2c3	904	55	0/0/0
4444.4444.4444.00-00	0x00000012	0x35f6	1002	131	0/0/0

Total LSP(s): 5

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),

ATT-Attached, P-Partition, OL-Overload

Směrovač R3H – Huawei:

- **Výpis konfigurace IS-IS:**

```
[R3H]display current-configuration
[V200R003C00SPC200]
#
 sysname R3H
#
ipv6
#
isis 1
 is-level level-2
 network-entity 49.0020.3333.3333.3333.00
 #
 ipv6 enable topology standard
 #
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 4::1/64
 isis ipv6 enable 1
 isis authentication-mode simple plain Test
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 3::2/64
 isis ipv6 enable 1
 isis authentication-mode simple plain Test
#
return
```

- **Výpis směrovací tabulky:**

```
[R3H]dis ipv6 routing-table
Routing Table : Public
        Destinations : 11       Routes : 11

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : FE80::A19:A6FF:FE9B:6D4F     Preference   : 15
 Cost         : 30                           Protocol     : ISIS-L2
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1         Flags        : D

 Destination  : 2::                          PrefixLength : 64
 NextHop      : FE80::A19:A6FF:FE9B:6D4F     Preference   : 15
 Cost         : 20                           Protocol     : ISIS-L2
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1         Flags        : D

 Destination  : 3::                          PrefixLength : 64
 NextHop      : 3::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1         Flags        : D

 Destination  : 3::2                         PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
```

```
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1       Flags        : D

Destination  : 4::                        PrefixLength : 64
NextHop      : 4::1                       Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 4::1                       PrefixLength : 128
NextHop      : ::1                        Preference   : 0
Cost         : 0                          Protocol     : Direct
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 5::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5820   Preference   : 15
Cost         : 20                         Protocol     : ISIS-L2
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 6::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5820   Preference   : 15
Cost         : 20                         Protocol     : ISIS-L2
RelayNextHop : ::                         TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0       Flags        : D

Destination  : 7::                        PrefixLength : 64
NextHop      : FE80::217:5AFF:FE4B:5820   Preference   : 15
Cost         : 30                         Protocol     : ISIS-L2
```

```
 RelayNextHop : ::                          TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0        Flags        : D

 Destination  : FE80::                      PrefixLength : 10
 NextHop      : ::                          Preference   : 0
 Cost         : 0                           Protocol     : Direct
 RelayNextHop : ::                          TunnelID     : 0x0
 Interface    : NULL0                       Flags        : D
```

- **Výpis databáze LS:**

```
[R3H]dis isis lsdb

                      Database information for ISIS(1)
                      --------------------------------

                        Level-2 Link State Database

LSPID                 Seq Num  Checksum Holdtime Length ATT/P/OL
-------------------------------------------------------------------------------
2222.2222.2222.00-00  0x0000001b 0xf04a 454      132     0/0/0
2222.2222.2222.02-00  0x00000008 0x35c3 454       55     0/0/0
3333.3333.3333.00-00* 0x00000014 0xde80 751      129     0/0/0
3333.3333.3333.02-00* 0x00000008 0x2c3  750       55     0/0/0
4444.4444.4444.00-00  0x00000012 0x35f6 849      131     0/0/0

Total LSP(s): 5
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self
LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload
```

Směrovač R4C – Cisco:

- **Výpis konfigurace IS-IS:**

```
R4C#show running-config
version 12.3
!
hostname R4C
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 4::2/64
 ipv6 enable
 ipv6 router isis 1
 isis password Test
!
interface FastEthernet0/1
 duplex auto
 speed auto
 ipv6 address 5::1/64
 ipv6 enable
 ipv6 router isis 1
 isis password Test
!
router isis 1
 net 49.0030.4444.4444.4444.00
!
line con 0
 logging synchronous
```

- **Výpis směrovací tabulky:**

```
R4C#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS -
ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I2  1::/64 [115/40]
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
I2  2::/64 [115/30]
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
I2  3::/64 [115/20]
     via FE80::A19:A6FF:FE9A:8276, FastEthernet0/0
C   4::/64 [0/0]
     via ::, FastEthernet0/0
L   4::2/128 [0/0]
     via ::, FastEthernet0/0
C   5::/64 [0/0]
     via ::, FastEthernet0/1
L   5::1/128 [0/0]
     via ::, FastEthernet0/1
I1  6::/64 [115/10]
     via FE80::A19:A6FF:FE9B:B705, FastEthernet0/1
I1  7::/64 [115/20]
     via FE80::A19:A6FF:FE9B:B705, FastEthernet0/1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

- **Výpis sousedních vazeb:**

```
R4C#show isis neighbors


System Id      Type Interface IP Address      State Holdtime
Circuit Id
3333.3333.3333 L2   Fa0/0                     UP    8
3333.3333.3333.02
5555.5555.5555 L1   Fa0/1                     UP    7
5555.5555.5555.01
```

Příloha D: *Konfigurace a výpisy ke kapitole 3.4 Směrování pomocí BGP4+*

Tato příloha obsahuje konfiguraci a důležité výpisy z vybraných zařízení. Především se jedná o alespoň jedno zařízení od každého výrobce, popř. ostatních zařízení, které v konfiguraci hrály nezbytnou roli. Některé konfigurační výpisy byly zkrácené z důvodu příliš zdlouhavého výpisu.

Směrovač R2H – Huawei:

- **Výpis konfigurace BGP4+:**

```
[R2H]display current-configuration
[V200R005C20SPC200]
#
 sysname R2H
#
ipv6
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 1::2/64
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 2::1/64
#
interface GigabitEthernet0/0/2
 ipv6 enable
 ipv6 address 3::1/64
#
bgp 65011
 router-id 2.2.2.2
 peer 1::1 as-number 65010
 peer 2::2 as-number 65011
 peer 3::2 as-number 65011
 #
```

```
 ipv4-family unicast
  undo synchronization
 #
 ipv6-family unicast
  undo synchronization
  network 1:: 64
  network 2:: 64
  network 3:: 64
  peer 1::1 enable
  peer 2::2 enable
  peer 3::2 enable
#
return
```

- **Výpis směrovací tabulky:**

```
[R2H]dis ipv routing-table
Routing Table : Public
        Destinations : 12       Routes : 12

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : 1::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D
```

```
Destination  : 1::2                          PrefixLength : 128
NextHop      : ::1                           Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0          Flags        : D

Destination  : 2::                           PrefixLength : 64
NextHop      : 2::1                          Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : D

Destination  : 2::1                          PrefixLength : 128
NextHop      : ::1                           Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : D

Destination  : 3::                           PrefixLength : 64
NextHop      : 3::1                          Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2          Flags        : D

Destination  : 3::1                          PrefixLength : 128
NextHop      : ::1                           Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2          Flags        : D

Destination  : 4::                           PrefixLength : 64
```

```
NextHop      : 2::2                          Preference   : 255
Cost         : 0                             Protocol     : IBGP
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : RD

Destination  : 5::                           PrefixLength : 64
NextHop      : 1::1                          Preference   : 255
Cost         : 0                             Protocol     : EBGP
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0          Flags        : D

Destination  : 6::                           PrefixLength : 64
NextHop      : 2::2                          Preference   : 255
Cost         : 0                             Protocol     : IBGP
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : RD

Destination  : 7::                           PrefixLength : 64
NextHop      : 3::2                          Preference   : 255
Cost         : 0                             Protocol     : IBGP
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2          Flags        : RD

Destination  : FE80::                        PrefixLength : 10
NextHop      : ::                            Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : NULL0                         Flags        : D
```

Směrovač R1C – Cisco:

- **Výpis konfigurace BGP4+:**

```
R1C#show running-configuration
!
version 12.4
!
hostname R1C
!
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 1::1/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 5::1/64
 ipv6 enable
!
router bgp 65010
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 1::2 remote-as 65011
 !
```

```
 address-family ipv6
  neighbor 1::2 activate
  network 1::/64
  network 5::/64
 exit-address-family
!
line con 0
 logging synchronous
```

- **Výpis směrovací tabulky:**

```
R1C#show ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route, B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1, I2 - ISIS L2,
IA - ISIS interarea, IS - ISIS summary, D – EIGRP, EX - EIGRP
external, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2
- OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   1::/64 [0/0] via FastEthernet0/0, directly connected
L   1::1/128 [0/0] via FastEthernet0/0, receive
B   2::/64 [20/0] via 1::2
B   3::/64 [20/0] via 1::2
B   4::/64 [20/0] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
C   5::/64 [0/0] via FastEthernet0/1, directly connected
L   5::1/128 [0/0] via FastEthernet0/1, receive
B   6::/64 [20/0] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
B   7::/64 [20/0] via FE80::A19:A6FF:FE9B:6D4E, FastEthernet0/0
L   FF00::/8 [0/0] via Null0, receive
```

- **Výpis sousedních BGP směrovačů:**

```
R1C#sh bgp ipv6 unicast neighbors
BGP neighbor is 1::2,  remote AS 65011, external link
  BGP version 4, remote router ID 2.2.2.2
```

```
  BGP state = Established, up for 00:51:54
  Last read 00:00:54, last write 00:00:33, hold time is 180,
keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv6 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1         13
    Keepalives:            52         52
    Route Refresh:          0          0
    Total:                 54         66
  Default minimum time between advertisement runs is 30 seconds
```

Směrovač R3H – Huawei:

- **Výpis konfigurace BGP4+:**

```
[R3H]dis current-configuration
[V200R003C00SPC200]
#
 sysname R3H
#
ipv6
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 4::1/64
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address 2::2/64
#
interface GigabitEthernet0/0/2
 ipv6 enable
 ipv6 address 6::1/64
#
bgp 65011
 router-id 3.3.3.3
 peer 2::1 as-number 65011
 peer 4::2 as-number 65011
 #
 ipv4-family unicast
  undo synchronization
 #
 ipv6-family unicast
  undo synchronization
```

```
  network 2:: 64
  network 4:: 64
  network 6:: 64
  peer 2::1 enable
  peer 4::2 enable
#
return
```

- **Výpis směrovací tabulky:**

```
[R3H]dis ipv routing-table
Routing Table : Public
        Destinations : 12       Routes : 12

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : 2::1                         Preference   : 255
 Cost         : 0                            Protocol     : IBGP
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1         Flags        : RD

 Destination  : 2::                          PrefixLength : 64
 NextHop      : 2::2                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1         Flags        : D
```

```
Destination  : 2::2                          PrefixLength : 128
NextHop      : ::1                           Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : D

Destination  : 3::                           PrefixLength : 64
NextHop      : 2::1                          Preference   : 255
Cost         : 0                             Protocol     : IBGP
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : RD

Destination  : 4::                           PrefixLength : 64
NextHop      : 4::1                          Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0          Flags        : D

Destination  : 4::1                          PrefixLength : 128
NextHop      : ::1                           Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0          Flags        : D

Destination  : 5::                           PrefixLength : 64
NextHop      : 1::1                          Preference   : 255
Cost         : 0                             Protocol     : IBGP
RelayNextHop : 2::1                          TunnelID     : 0x0
Interface    : GigabitEthernet0/0/1          Flags        : RD

Destination  : 6::                           PrefixLength : 64
```

```
NextHop      : 6::1                          Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2          Flags        : D

Destination  : 6::1                          PrefixLength : 128
NextHop      : ::1                           Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/2          Flags        : D

Destination  : 7::                           PrefixLength : 64
NextHop      : 4::2                          Preference   : 255
Cost         : 0                             Protocol     : IBGP
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : GigabitEthernet0/0/0          Flags        : RD

Destination  : FE80::                        PrefixLength : 10
NextHop      : ::                            Preference   : 0
Cost         : 0                             Protocol     : Direct
RelayNextHop : ::                            TunnelID     : 0x0
Interface    : NULL0                         Flags        : D
```

- **Výpis sousedních BGP směrovačů:**

```
[R3H]dis bgp ipv peer

 BGP local router ID : 3.3.3.3
 Local AS number : 65011
 Total number of peers : 2        Peers in established state : 2

  Peer V    AS MsgRcvd MsgSent OutQ  Up/Down       State PrefRcv

  2::1 4 65011      86      79    0 01:14:20 Established       4
  4::2 4 65011      74      68    0 01:03:45 Established       3
```

Příloha E: *Konfigurace a výpisy ke kapitole 4.1 IPv6 přes IPv4 manuální GRE tunel*

Tato příloha obsahuje konfiguraci a důležité výpisy z vybraných zařízení. Především se jedná o alespoň jedno zařízení od každého výrobce, popř. ostatních zařízení, které v konfiguraci hrály nezbytnou roli. Některé konfigurační výpisy byly zkrácené z důvodu příliš zdlouhavého výpisu.

Směrovač R1H – Huawei:

- **Výpis konfigurace:**

```
[R1H]display current-configuration
[V200R005C20SPC200]
#
 sysname R1H
#
ipv6
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 10.1.1.1 255.255.255.0
 ipv6 address 1::1/64
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.252
#
interface Tunnel0/0/1
 ipv6 enable
 ipv6 address 3::1/64
 tunnel-protocol gre
 source 10.0.0.1
 destination 10.0.0.6
#
ospf 1
```

```
 area 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 10.1.1.0 0.0.0.255
#
ipv6 route-static 2:: 64 Tunnel0/0/1
#
Return
```

- **Výpis směrovací tabulky:**

```
[R1H]display ipv6 routing-table
Routing Table : Public
        Destinations : 7        Routes : 7

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : 1::                          PrefixLength : 64
 NextHop      : 1::1                         Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D

 Destination  : 1::1                         PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0         Flags        : D
```

```
Destination  : 2::                    PrefixLength : 64
NextHop      : 3::1                   Preference   : 60
Cost         : 0                      Protocol     : Static
RelayNextHop : ::                     TunnelID     : 0x0

Interface    : Tunnel0/0/1            Flags        : D
Destination  : 3::                    PrefixLength : 64
NextHop      : 3::1                   Preference   : 0
Cost         : 0                      Protocol     : Direct
RelayNextHop : ::                     TunnelID     : 0x0
Interface    : Tunnel0/0/1            Flags        : D

Destination  : 3::1                   PrefixLength : 128
NextHop      : ::1                    Preference   : 0
Cost         : 0                      Protocol     : Direct
RelayNextHop : ::                     TunnelID     : 0x0
Interface    : Tunnel0/0/1            Flags        : D

Destination  : FE80::                 PrefixLength : 10
NextHop      : ::                     Preference   : 0
Cost         : 0                      Protocol     : Direct
RelayNextHop : ::                     TunnelID     : 0x0
Interface    : NULL0                  Flags        : D
```

Směrovač R3C – Cisco:

- **Výpis konfigurace:**

```
R3C#show running-config

version 12.4
!
hostname R3C
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
interface Tunnel1
 no ip address
 ipv6 address 3::2/64
 tunnel source 10.0.0.6
 tunnel destination 10.0.0.1
!
interface FastEthernet0/0
 ip address 10.0.0.6 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.2.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 enable
!
router ospf 1
```

```
 log-adjacency-changes
 network 10.0.0.4 0.0.0.3 area 0
 network 10.1.2.0 0.0.0.255 area 0
!
!
ipv6 route 1::/64 Tunnel1
!
line con 0
 logging synchronous
end
```

- **Výpis směrovací tabulky:**

```
R3C#show ipv6 route
IPv6 Routing Table - Default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route, B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1, I2 - ISIS L2,
IA - ISIS interarea, IS - ISIS summary, D – EIGRP, EX - EIGRP
external ,O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2
- OSPF ext 2 ,ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   1::/64 [1/0] via Tunnel1, directly connected
C   2::/64 [0/0] via FastEthernet0/1, directly connected
L   2::1/128 [0/0] via FastEthernet0/1, receive
C   3::/64 [0/0] via Tunnel1, directly connected
L   3::2/128 [0/0] via Tunnel1, receive
L   FF00::/8 [0/0] via Null0, receive
```

- **Výpis informací o tunelu:**

```
R3C#show interface tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 2/255, rxload 2/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.6, destination 10.0.0.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
```